边缘计算安全白皮书

边缘计算产业联盟（ECC）与工业互联网产业联盟（AII）联合发布
2019 年 11 月

边缘计算 Edge Computing CONSORTIUM
工业互联网产业联盟 Alliance of Industrial Internet

指导单位：

工业和信息化部网络安全管理局

参与编写单位：

中国科学院沈阳自动化研究所
华为技术有限公司
北京奇安信科技有限公司
北京神州绿盟信息安全科技股份有限公司
北京大学
北京和利时系统工程有限公司
中国联通研究院
国家工业信息安全发展研究中心
航天云网科技发展有限责任公司
石化盈科信息技术有限责任公司
盛科网络（苏州）有限公司
西安电子科技大学
华中科技大学
中山大学
阿里巴巴网络技术有限公司
国网辽宁省电力有限公司电力科学研究院
中国南方电网有限责任公司

编写组成员：

于海斌、曾鹏、尚文利、翁志强、黄还青、陈春雨、陶耀东、王晓鹏、沈晴霓、邓良、李俊、徐伟、张华、张国颖、穆雷霆、王冲华、程中林、徐雷、于城、裴庆祺、胡晓娅、周纯杰、刘一涛、董之微、李桐、许爱东、蒋屹新、张宇南、崔君荣、陈旭、谭晓军、赵剑明、刘贤达、尹隆、佟国毓、李越、程晓磊

PREFACE 前言

边缘计算已受到学术界、产业界以及政府部门的极大关注，正在从产业共识走向了产业实践，在电力、交通、制造、智慧城市等多个价值行业有了规模应用，产业界在实践中逐步认识到边缘计算的本质与核心能力。

伴随行业数字化转型进程的不断深入，边缘计算网络架构的变迁必然导致针对云边缘、边缘云、云化网关等边缘计算节点的安全攻击不断增多，边缘安全问题已成为限制边缘计算产业发展的障碍之一。

为加速并保障边缘计算产业的发展，提升典型价值场景下的边缘安全保障能力，边缘计算产业联盟（Edge Computing Consortium，缩写为 ECC）与工业互联网产业联盟（Alliance of Industrial Internet，缩写为 AII）共同研究编写边缘计算安全白皮书。作为《边缘计算参考架构 3.0》的延伸，许多重要的术语和概念与其保持一致，本文档不再一一详细说明，读者可以参考《边缘计算参考架构 3.0》的相关内容。

本白皮书目的是识别、解释和定位与边缘安全相关的体系结构、设计和技术，从边缘安全的重要性和价值出发，分析了典型价值场景下边缘安全面临的挑战和需求特征，并提出了边缘安全的参考框架和确保处理相应安全问题的方法组合。

本文档的目标读者包括但不限于边缘计算产业联盟的所有成员，联盟成员的供应商，安全产品提供商，安全服务提供商，系统集成商以及其他关心边缘计算系统安全相关的机构和个人。

CONTENTS

目录

前言

1. 边缘安全保障并加速边缘计算落地实践 01

1.1 边缘计算 2.0 01

1.2 边缘计算参考架构 3.0 02

1.3 边缘安全重要性和价值 03

1.4 边缘安全白皮书的内容和范畴 03

2. 边缘安全挑战及需求特征 04

2.1 边缘安全十二大挑战 04

2.2 边缘安全的五大需求特征 09

2.3 边缘安全的边界 11

3. 边缘安全参考框架 12

3.1 多视图呈现 13

3.2 边缘安全十大关键技术 24

4. 典型场景下的边缘安全案例 26

4.1 智能制造领域边云协同场景下的典型安全解决方案 26

4.2 泛终端安全准入典型案例 28

4.3 自动驾驶边缘安全案例 30

4.4 C2M- 家具定制行业 - 边缘安全解决方案 32

附录 1：术语表 34

附录 2：缩略语表 36

附录 3：参考文献 39

01

边缘安全保障并加速边缘计算落地实践

1.1 边缘计算 2.0

边缘计算产业联盟（ECC）2017 年发布的《边缘计算参考架构 1.0》中给出了边缘计算 1.0 的定义。边缘计算是在靠近物或数据源头的网络边缘侧，融合网络、计算、存储、应用核心能力的开放平台，就近提供边缘智能服务，满足行业数字化在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求。它从边缘计算的位置、能力与价值等维度给出定义，在边缘计算产业发展的初期有效牵引产业共识，推动边缘计算产业的发展。

随着边缘计算产业的发展逐步从产业共识走向落地实践，边缘计算的主要落地形态、技术能力发展方向、软硬件平台的关键能力等问题逐渐成为产业界的关注焦点，边缘计算 2.0 应运而生。

边缘计算 2.0：边缘计算的业务本质是云计算在数据中心之外汇聚节点的延伸和演进，主要包括云边缘、边缘云和云化网关三类落地形态；以“边云协同”和“边缘智能”为核心能力发展方向；软件平台需要考虑导入云理念、云架构、云技术，提供端到端实时、协同式智能、可信赖、可动态重置等能力；硬件平台需要考虑异构计算能力，如鲲鹏、ARM、X86、GPU、NPU、FPGA 等。

云边缘：云边缘形态的边缘计算，是云服务在边缘侧的延伸，逻辑上仍是云服务，主要的能力提供依赖于云服务或需要与云服务紧密协同。如华为云提供的 IEF 解决方案、阿里云提供的 Link Edge 解决方案、AWS 提供的 Greengrass 解决方案等均属于此类。

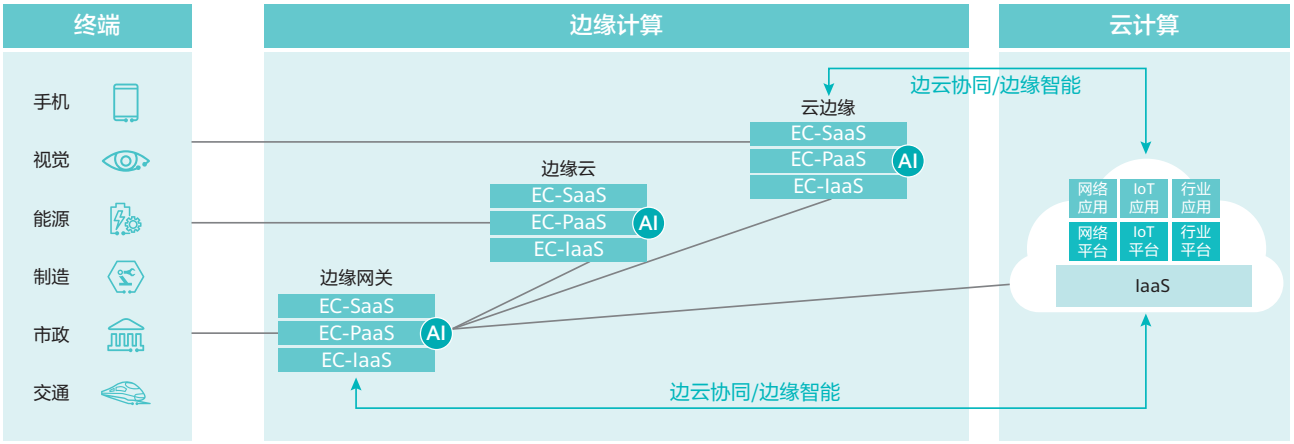


图 1 边缘计算 2.0

边缘云：边缘云形态的边缘计算，是在边缘侧构建中小规模云服务能力，边缘服务能力主要由边缘云提供；集中式 DC 侧的云服务主要提供边缘云的管理调度能力。如多接入边缘计算（MEC）、CDN、华为云提供的 IEC 解决方案等均属于此类。

云化网关：云化网关形态的边缘计算，以云化技术与能力重构原有嵌入式网关系统，云化网关在边缘侧提供协议 / 接口转换、边缘计算等能力，部署在云侧的控制器提供边缘节点的资源调度、应用管理与业务编排等能力。

1.2 边缘计算参考架构 3.0

基于模型驱动的工程方法（Model-Driven Engineering MDE），ECC 2018 年提出了边缘计算参考架构 3.0。参考架构 3.0 在每层提供了模型化的开放接口，实现了架构的全层次开放；通过纵向管理服务、数据全生命周期服务、安全服务，实现业务的全流程、全生命周期的智能服务。

边缘计算参考架构 3.0 的主要内容包括：

» 整个系统分为云、边缘和现场三层，边缘计算位于云和现场层之间，边缘层向下支持各种现场设备的接入，向上可以与云端对接；

» 边缘层包括边缘节点和边缘管理器两个主要部分。边缘节点是硬件实体，是承载边缘计算业务的核心。边缘管理器的呈现核心是软件，主要功能是对边缘节点进行统一的管理；

» 边缘计算节点一般具有计算、网络和存储资源，边缘计算系统对资源的使用有两种方式：第一，直接将计算、网络和存储资源进行封装，提供调用接口，边缘管理器以代码下载、网络策略配置和数据库操作等方式使用边缘节点资源；第二，进一步将边缘节点的资源按功能领域封装成功能模块，边缘管理器通过模型驱动的业务编排的方式组合和调用功能模块，实现边缘计算业务的一体化开发和敏捷部署。

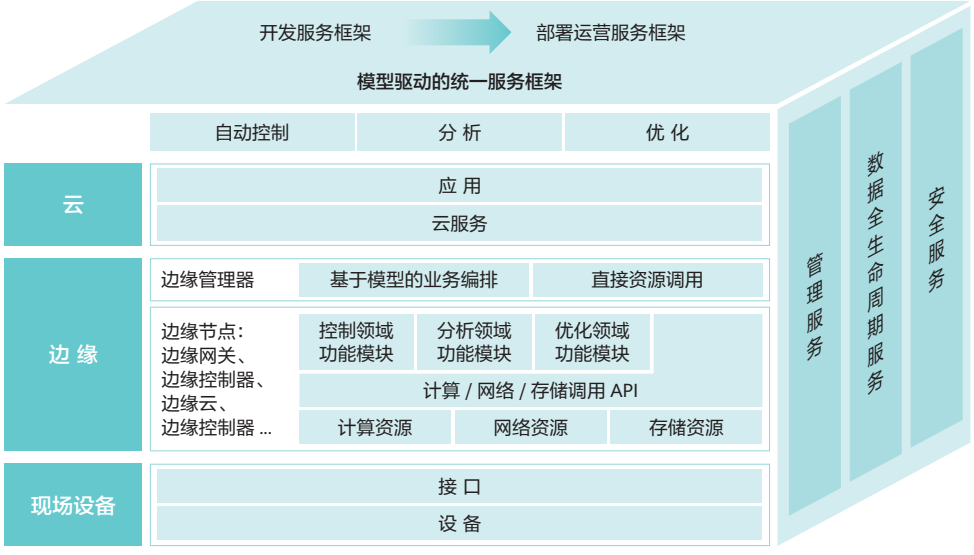


图 2 边缘计算参考架构 3.0

1.3 边缘安全重要性和价值

边缘计算的CROSS (Connectivity、Realtime、data Optimization、Smart、Security) 价值推动计算模型从集中式的云计算走向更加分布式的边缘计算，为传统的网络架构带来了极大的改变，这些改变促进了技术和业务的发展，同时也将网络攻击威胁引入了网络边缘。以工业场景为例，根据《中国工业互联网安全态势报告》，截至2018年11月，全球范围内暴露在互联网上的工控系统及设备数量已超10万台。

边缘安全是边缘计算的重要保障。边缘安全涉及跨越云计算和边缘计算纵深的安全防护体系，增强边缘基础设施、网络、应用、数据识别和抵抗各种安全威胁的能力，为边缘计算的发展构建安全可信环境，加速并保障边缘计算产业发展。

边缘安全的价值体现在下述几方面：

提供可信的基础设施：主要包括了计算、网络、存储类的物理资源和虚拟资源。基础设施是包含路径、数据交互和处理模型的平台面，应对镜像篡改、DDoS攻击、非授权通信访问、端口入侵等安全威胁。

为边缘应用提供可信赖的安全服务：从运行维护角度，提供应用监控、应用审计、访问控制等安全服务；从数据安全角度，提供轻量级数据加密、数据安全存储、敏感数据处理与监测的安全服务，进一步保证应用业务的数据安全。

保障安全的设备接入和协议转换：边缘计算节点数量庞大，面向工业行业存在中心云、边缘云、边缘网关、边缘控制器等多种终端和边缘计算形态，复杂性异构性突出。保证安全的接入和协议转换，有助于为数据提供存储安全、共享安全、计算安全、传播和管控以及隐私保护。

提供安全可信的网络及覆盖：安全可信的网络除了传统的运营商网络安全保障（如：鉴权、秘钥、合法监听、防火墙技术）以外，目前面向特定行业的TSN、工业专网等，也需要定制化的网络安全防护。

提供端到端全覆盖的包括威胁监测、态势感知、安全管理编排、安全事件应急响应、柔性防护在内的全网安全运营防护体系。

1.4 边缘安全白皮书的内容和范畴

本白皮书聚焦边缘计算相关的安全能力构建。

安全涉及到Security、Safety、Privacy、Trust等方面，由于Safety有相对独立的标准规范体系，本白皮书将主要涉及边缘侧的Security、Privacy、Trust等维度，而不以Safety为重点。

本白皮书围绕工业边缘计算、企业与IoT边缘计算、电信运营商三大典型边缘计算价值场景，综合运用信息安全、功能安全、可信、边云协同等技术手段，分析边缘安全面临的挑战和以及需求特征，并分别在边缘基础设施、边缘网络、边缘数据、边缘应用、边缘全生命周期、边云协同等维度提出了相应的安全防护措施。

本白皮书以推动边缘安全的产业共识为目标，为相关产业生态链构建和使用相关能力提供参考借鉴。

02

边缘安全挑战及需求特征

2.1 边缘安全十二大挑战

当前产业界以及学术界已经开始认识到边缘安全的重要性和价值，并开展了积极有益的探索，但是目前关于边缘安全的探索仍处于产业发展的初期，缺乏系统性的研究。

本白皮书就边缘计算环境中潜在的攻击窗口进行分析，包括边缘接入（云 - 边接入，边 - 端接入），边缘服务器（硬件、软件、数据），边缘管理（账号、管理 / 服务接口、管理人员）等层面的攻击，如下图和下表所示，汇总编写了边缘计算面临的 12 个最重要的安全挑战。这 12 个安全挑战是依据调研的工业边缘计算、企业和 IoT 边缘计算企业的关注程度，从高到低排序，它们的顺序和具体描述如下：

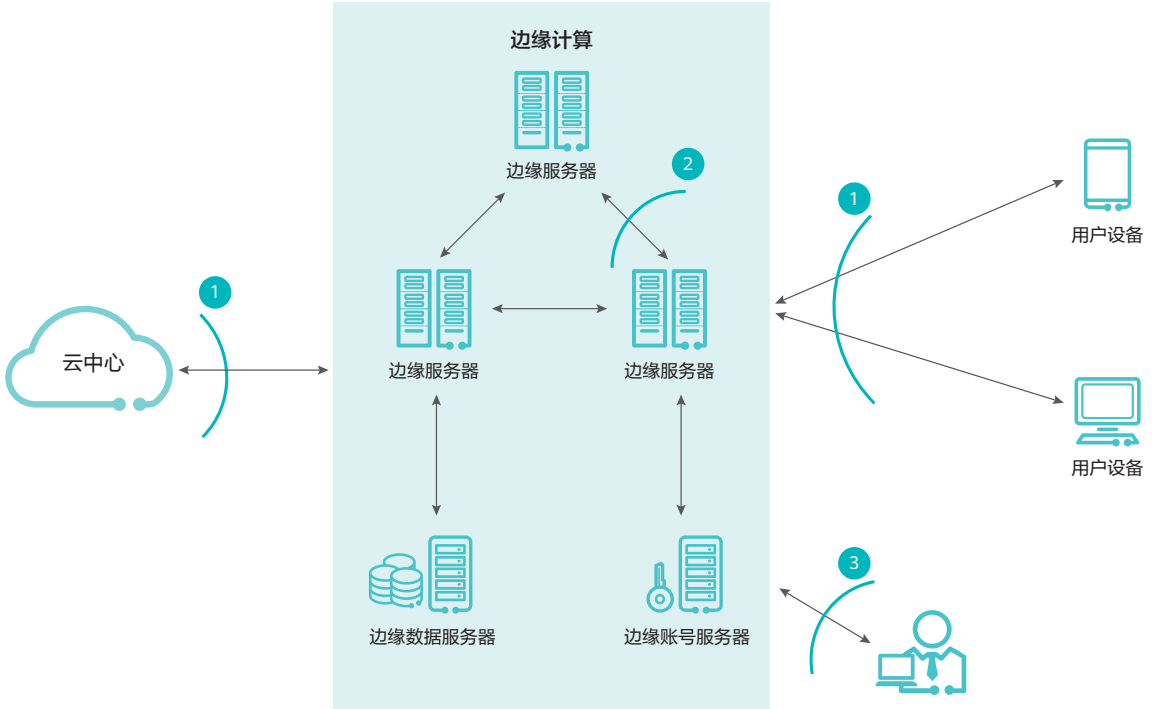


图 3 边缘计算环境中潜在的攻击窗口

攻击面	挑战
边缘接入	不安全的通信协议；恶意的边缘节点
边缘服务器	边缘节点数据易被损毁；隐私数据保护不足；不安全的系统与组件；易发起分布式拒绝服务；易蔓延 APT 攻击；硬件安全支持不足
边缘管理	身份、凭证和访问管理不足；账号信息易被劫持；不安全的接口和 API；难监管的恶意管理员

挑战 1：不安全的通信协议
Security, Privacy；边缘网络安全

场景描述：由于边缘节点与海量、异构、资源受限的现场 / 移动设备大多采用短距离的无线通信技术，边缘节点与云服务器采用的多是消息中间件或网络虚拟化技术，这些协议大多安全性考虑不足。比如，在工业边缘计算、企业和 IoT 边缘计算场景下，传感器与边缘节点之间存在着众多不安全的通信协议（如：ZigBee、蓝牙等），缺少加密、认证等措施，易于被窃听和篡改；在电信运营商边缘计算场景下，边缘节点与用户之间采用的是基于 WPA2 的无线通信协议，云服务器与边缘节点之间采用基于即时消息协议的消息中间件，通过网络 Overlay 控制协议对边缘的网络设备进行网络构建和扩展，考虑的主要是通信性能，对消息的机密性、完整性、真实性和不可否认性等考虑不足。

挑战 2：边缘节点数据易被损毁
Security, Trust；边缘数据安全

场景描述：由于边缘计算的基础设施位于网络边缘，缺少有效的数据备份、恢复、以及审计措施，导致攻击者可能修改或删除用户在边缘节点上的数据来销毁某些证据。在企业和 IoT 边缘计算场景下，以交通监管场景为例，路边单元上的边缘节点保存了附近车辆报告的交通事故视频，这是事故取证的重要证据。罪犯可能会攻击边缘节点伪造证据以摆脱惩罚。再者，在电信运营商边缘计算场景下，一旦发生用户数据在边缘节点 / 服务器上丢失或损坏，而云端又没有对应用户数据的备份，边缘节点端也没有提供有效机制恢复数据，则用户只能被迫接受这种损失；如果上述情况发生在工业边缘计算场景下，边缘节点上数据的丢失或损坏将直接影响批量的工业生产和决策过程。

挑战 3：隐私数据保护不足
Privacy, Security；边缘数据安全

场景描述：边缘计算将计算从云迁移到临近用户的一端，直接对数据进行本地处理和决策，在一定程度上避免了数据在网络中长距离的传播，降低了隐私泄露的风险。然而，由于边缘设备获取的是用户第一手数据，能够获得大量的敏感隐私数据。例如，在电信运营商边缘计算场景下，边缘节点的好奇用户极容易收集和窥探到其他用户的位置信息、服务内容和使用频率等。在工业边缘计算、企业和 IoT 边缘计算场景下，边缘节点相对于传统的云中心，缺少有效的加密或脱敏措施，一旦受到黑客攻击、嗅探和腐蚀，其存储的家庭人员消费、电子医疗系统中人员健康信息、道路事件车辆信息等将被泄露。

挑战 4：不安全的系统与组件
Security, Trust；边缘基础设施安全

场景描述：边缘节点可以分布式承担云的计算任务。然而，边缘节点的计算结果是否正确对用户和云来说都存在信任问题。在电信运营商边缘计算场景下，尤其是在工业边缘计算、企业和 IoT 边缘计算场景下，边缘节点可能从云端卸载的是不安全的定制操作系统，或者这些系统调用的是被敌手腐蚀了的供应链上的第三方软件或硬件组件。一旦攻击者利用边缘节点上不安全 Host OS 或虚拟化软件的漏洞攻击 Host OS 或利用 Guest OS，通过权限升级或者恶意软件入侵边缘数据中心，并获得系统的控制权限，则恶意用户可能会终止、篡改边缘节点提供的业务或返回错误的计算结果。如果不能提供有效机制验证卸载的系统和组件的完整性和计算结果的正确性，云可能不会将计算任务转移到边缘节点，用户也不会访问边缘节点提供的服务。

挑战 5：身份、凭证和访问管理不足
Security, Trust；边缘应用安全

场景描述：身份认证是验证或确定用户提供的访问凭证是否有效的过程。在工业边缘计算、企业和 IoT 边缘计算场景下，许多现场设备没有足够的存储和计算资源来执行认证协议所需的加密操作，需要外包给边缘节点，但这将带来一些问题：终端用户和边缘计算服务器之间必须相互认证，安全凭证如何产生和管理？在大规模、异构、动态的边缘网络中，如何在大量分布式边缘节点和云中心之间实现统一的身份认证和高效的密钥管理？在电信运营商边缘计算场景下，移动终端用户无法利用传统的 PKI 体制对边缘节点进行认证，加上具有很强的移动性，如何实现在不同边缘节点间切换时的高效认证？。此外，在边缘计算环境下，边缘服务提供商如何为动态、异构的大规模设备用户接入提供访问控制功能，并支持用户基本信息和策略信息的分布式的远程提供，以及定期更新。

挑战 6：账号信息易被劫持
Security；边缘网络安全

场景描述：账号劫持是一种身份窃取，主要目标一般为现场设备用户，攻击者以不诚实的方式获取设备或服务所绑定的用户特有的唯一身份标识。账号劫持通常通过钓鱼邮件、恶意弹窗等方式完成。通过这种方式，用户往往在无意中泄露自己的身份验证信息。攻击者以此来执行修改用户账号、创建新账号等恶意操作。在工业边缘计算、企业和 IoT 边缘计算场景下，用户的现场设备往往与固定的边缘节点直接相连，设备的账户通常采用的是弱密码、易猜测密码和硬编码密码，攻击者更容易伪装成合法的边缘节点对用户进行钓鱼、欺骗等操作。在电信运营商边缘计算场景，用户的终端设备经常需要在不同边缘节点之间移动和频繁地切换接入，攻击者很容易通过入侵用户已经经过的边缘节点，或者伪造成一个合法的边缘节点，截获或非法获取用户认证使用的账号信息。

挑战 7：恶意的边缘节点

Safety, Security, Trust；边缘基础设施安全

场景描述：在边缘计算场景下，参与实体类型多、数量大，信任情况非常复杂。攻击者可能将恶意边缘节点伪装成合法的边缘节点，诱使终端用户连接到恶意边缘节点，隐秘地收集用户数据。此外，边缘节点通常被放置在用户附近，在基站或路由器等位置，甚至在 WiFi 接入点的极端网络边缘，这使得为其提供安全防护变得非常困难，物理攻击更有可能发生。例如：在电信运营商边缘计算场景下，恶意用户可能在边缘侧部署伪基站、伪网关等设备，造成用户的流量被非法监听；在工业边缘计算场景下，边缘计算节点系统大多以物理隔离为主，软件安全防护能力更弱，外部的恶意用户更容易通过系统漏洞入侵和控制部分边缘节点，发起非法监听流量的行为等；在企业和 IoT 边缘计算场景下，边缘节点存在地理位置分散、暴露的情况，在硬件层面易受到攻击。由于边缘计算设备结构、协议、服务提供商的不同，现有入侵检测技术难以检测上述攻击。

挑战 8：不安全的接口和 API

Security；边缘应用安全

场景描述：在云环境下，为了方便用户与云服务交互，要开放一系列用户接口或 API 编程接口，这些接口需防止意外或恶意接入。此外，第三方通常会基于这些接口或 API 来开发更多有附加价值的服务，这就会引入新一层的更复杂的 API，同时风险也会相应的增加。因此，无论是在工业边缘计算、企业和 IoT 边缘计算场景下，还是在电信运营商边缘计算场景下，边缘节点既要向海量的现场设备提供接口和 API，又要与云中心进行交互，这种复杂的边缘计算环境、分布式的架构，引入了大量的接口和 API 管理，但目前的相关设计并没有都考虑安全特性。

挑战 9：易发起分布式拒绝服务
Security；边缘网络安全

场景描述：在工业边缘计算、企业和 IoT 边缘计算场景下，由于参与边缘计算的现场设备通常使用简单的处理器和操作系统，对网络安全不重视，或者因设备本身的计算资源和带宽资源有限，无法支持支持复杂的安全防御方案，导致黑客可以轻松对这些设备实现入侵，然后利用这些海量的设备发起超大流量的 DDoS 攻击。因此，对如此大量的现场设备安全的协调管理是边缘计算的一个巨大挑战。

挑战 10：易蔓延 APT 攻击
Security；边缘基础设施安全

场景描述：APT 攻击是一种寄生形式的攻击，通常在目标基础设施中建立立足点，从中秘密地窃取数据，并能适应防备 APT 攻击的安全措施。在边缘计算场景下，APT 攻击者首先寻找易受攻击的边缘节点，并试图攻击它们和隐藏自己。更糟糕的是，边缘节点往往存在许多已知和未知的漏洞，且存在与中心云端安全更新同步不及时的问题。一旦被攻破，加上现在的边缘计算环境对 APT 攻击的检测能力不足，连接上该边缘节点的用户数据和程序无安全性可言。比传统网络 APT 威胁更大的是，在工业边缘计算、企业和 IoT 边缘计算场景下，由于现场设备和网络的默认设置大多不安全，边缘中心又不能提供有效机制及时修改这些配置，使得 APT 攻击易感染面更大、传播性也更强，很容易蔓延到大量的现场设备和其他边缘节点。

挑战 11：难监管的恶意管理员
Trust, Security；边缘应用安全

场景描述：同云计算场景类似，在工业边缘计算、企业和 IoT 边缘计算、电信运营商边缘计算等场景下，信任情况更加复杂，而且管理如此大量的 IoT 设备 / 现场设备，对管理员来说都是一个巨大的挑战，很可能存在不可信 / 恶意的管理员。出现这种情况的一种可能是管理员账户被黑客入侵，另一种可能是管理员自身出于其它的目的盗取或破坏系统与用户数据。如果攻击者拥有超级用户访问系统和物理硬件的权限，他将可以控制边缘节点整个软件栈，包括特权代码，如容器引擎、操作系统内核和其他系统软件，从而能够重放、记录、修改和删除任何网络数据包或文件系统等。加上现场设备的存储资源有限，对恶意管理员的审计不足。

挑战 12：硬件安全支持不足
Security, Trust；边缘基础设施安全

场景描述：相比于云计算场景，在工业边缘计算、企业和 IoT 边缘计算、电信运营商边缘计算等场景下，边缘节点远离云中心的管理，被恶意入侵的可能性大大增加，而且边缘节点更倾向于使用轻量级容器技术，但容器共享底层操作系统，隔离性更差，安全威胁更加严重。因此，仅靠软件来实现安全隔离，很容易出现内存泄露或篡改等问题。基于硬件的可信执行环境 TEEs（如 Intel SGX, ARM TrustZone, and AMD 内存加密技术等）目前在云计算环境已成为趋势，但是 TEEs 技术在工业边缘计算、企业和 IoT 边缘计算、电信运营商边缘计算等复杂信任场景下的应用，目前还存在性能问题，在侧信道攻击等安全性上的不足仍有待探索。

2.2 边缘安全的五大需求特征

边缘计算作为一种新的技术理念重新定义了企业信息系统中云、管、端的关系，边缘计算不是单一的部件，也不是单一的层次，而是涉及到 EC-IaaS、EC-PaaS、EC-SaaS 的端到端开放平台。边缘计算网络架构的变迁必然也对安全提出了与时俱进的需求，为了支撑边缘计算环境下的安全防护能力，边缘安全需要满足如下的需求特征：

2.2.1 海量特征

包括海量的边缘节点设备、海量的连接、海量的数据，围绕海量特征，边缘安全需要考虑下述特性与能力构建：

» **高吞吐：**由于边缘网络中连接的设备数量大、物理连接条件和连接方式多样，有些具有移动性，接入和交互频繁，要求相关的安全服务突破接入延迟和交互次数限制，即边缘节点的安全接入服务应具有高吞吐量。可采用的解决方案包括支持轻量级加密的安全接入协议，支持无缝切换接入的动态高效认证方案。

» **可扩展：**随着边缘网络中接入设备数量剧增，设备上运行着多样的应用程序并生成大量的数据，要求相关安全服务能够突破可支持的最大接入规模限制，即边缘节点的资源管理服务应具有可扩展性。可采用的解决方案包括物理资源虚拟化、跨平台资源整合、支持不同用户请求的资源之间安全协作和互操作等。

» **自动化：**由于边缘网络中海量的设备上运行着多样化的系统软件与应用程序，安全需求也多样化，要求相关安全服务能够突破管理人员限制，即边缘侧的设备安全管理应具有自动化。可采用的解决方案包括边缘节点对连接的设备实现自动化的安全配置、自动化的远程软件升级和更新、自动化的入侵检测等。

» **智能化：**由于边缘网络中接入设备数量大，生成和存储大量的数据，可以弥补云中心大数据分析时延性高、周期性长、网络耗能严重等缺陷，要求相关安全服务能够突破数据处理能力限制，即边缘节点的安全服务

应具有智能。可采用的解决方案包括云边协同的安全存储 / 安全多方计算、差分隐私保护等。

2.2.2 异构特征

包括计算的异构性、平台的异构性、网络的异构性以及数据的异构性，围绕异构特征，边缘安全需要考虑下述特性与能力构建：

» **无缝对接：**边缘网络中存在大量异构的网络连接和平台，边缘应用中也存在大量的异构数据，要求相关安全服务能够突破无缝对接限制，提供统一的安全接口，包括网络接入、资源调用和数据访问接口。可采用的解决方案：基于软件定义思想实现硬件资源的虚拟化和管理功能的可编程，即将硬件资源抽象为虚拟资源，提供标准化接口对虚拟资源进行统一安全管理和调度，实施统一的接入认证和 API 访问控制。

» **互操作：**边缘设备具有多样性和异构性，在无线信号、传感器、计算能耗、存储等方面具有不同的能力，通常会产生不可忽略的开销，并产生实现 / 操作复杂性。要求相关安全服务能够突破互操作性限制，提供设备的注册和标识，可采用的解决方案包括设备的统一安全标识，资源的发现、注册和安全管理等。

» **透明：**由于边缘设备的硬件能力和软件类型呈多样化，安全需求也呈多样化，要求相关安全服务能够突破对复杂设备类型管理能力的限制，即边缘节点对不同设备安全机制的配置应具有透明性。可采用的解决方案包括边缘节点可对不同设备安全威胁实现自动识别、安全机制的自动部署、安全策略的自动更新等。

2.2.3 资源约束特征

包括计算资源约束、存储资源约束以及网络资源约束，从而带来安全功能和性能上的约束。围绕资源约束特征，边缘安全需要考虑下述特性与能力构建：

» **轻量化：**由于边缘节点通常采用低端设备，存在计算、存储和网络资源受限、不支持额外的硬件安全特性（如 TPM、HSM、SGX enclave、硬件虚拟化等）限制，现有云安全防护技术并不能完全适用，需要提供轻量级的认证协议、系统安全加固、数据加密和隐私保护、以及硬件安全特性软件模拟方法等技术。

» **云边协同：**由于边缘节点的计算和存储资源受限，存在可管理的边缘设备规模和数据规模限制，且许多终端设备具有移动性（如车联网等），脱离云中心将无法为这些设备提供全方位的安全防护，需要提供云边协同的身份认证、数据备份和恢复、联合机器学习隐私保护、入侵检测等技术。

2.2.4 分布式特征

边缘计算更靠近用户侧，天然具备分布式特征。围绕分布式特征，边缘安全需要考虑下述特性与能力构建：

» **自治：**与传统云中心化管理不同，边缘计算具有多中心、分布式特点，因而在脱离云中心的离线情况下，可以损失部分安全能力，进行安全自治，或者说具有本地存活的能力。需要提供设备的安全识别、设备资源的安全调度与隔离、本地敏感数据的隐私保护、本地数据的安全存储等功能。

» **边边协同：**由于边缘计算的分布式特性，加上现场设备的移动性（经过多个边缘计算节点，甚至跨域 / 多边

缘中心）、以及现场环境 / 事件的变化，使得服务的需求（如智能交通）也发生变化，因此在安全方面也需要提供边边协同的安全策略管理。

» **可信硬件支持：**边缘节点连接的设备（如移动终端、IoT 设备）主要是无线连接和具有移动性，会出现频繁的、跨边缘节点的接入或退出情况，导致不断变化的拓扑和通信条件，松耦合和不稳定的架构，易受账号劫持、不安全系统与组件等威胁，需要提供轻量级可信硬件支持的强身份认证、完整性验证与恢复等。

» **自适应：**边缘节点动态地无线连接大量、不同类型的设备，每个设备上嵌入或安装了不同的系统、组件和应用程序，它们具有不同的生命周期和服务质量（QoS）要求，使得对边缘节点资源的需求和安全的需求也发生动态变化。需要提供灵活的安全资源调度、多策略的访问控制、多条件加密的身份认证方案等。

2.2.5 实时性特征

边缘计算更靠近用户侧，能够更好的满足实时性应用和服务的需求。围绕实时性特征，边缘安全需要考虑下述特性与能力构建：

» **低延迟：**边缘计算能够降低服务延迟，但是许多边缘计算场景（如工业、物联网等）仅能提供时间敏感服务，专有的网络协议或规约在设计时通常只强调通信的实时性及可用性，对安全性普遍考虑不足，安全机制的增加必将对工业实时性造成影响。需要提供轻量级、低延迟的安全通信协议。

» **容错：**边缘节点可以收集、存储与其连接现场设备的数据，但是缺乏数据备份机制，数据的不可用将直接影响服务的实时性。需要提供轻量级、低时延的数据完整性验证和恢复机制，以及高效的冗余备份机制，确保设备故障或数据损坏、丢失时，能够在限定的时间内快速恢复受影响 / 被损毁数据的可用性。

» **弹性：**边缘计算节点和现场设备均容易受到各种攻击，需要经常对系统、组件和应用程序进行升级和维护，但这将直接影响服务的实时性。需要提供支持业务连续性的软件在线升级和维护、系统受到攻击或破坏后的动态可信恢复机制。

2.3 边缘安全的边界

区别于云安全，边缘安全需求具备海量、异构、资源约束、分布式、实时性等特征。因此只有考虑了上述需求特征，且面向边缘计算的安全才属于边缘安全的范畴。

03

边缘安全参考框架

为了应对上述边缘安全面临的挑战，同时满足相应的安全需求和特征，需要提供相应的参考框架和关键技术，且参考框架需要拥有如下的能力：

» 安全功能适配边缘计算的特定架构，且能够灵活部署与扩展；
» 能够容忍一定程度和范围内的功能失效，但基础功能始终保持运行，且整个系统能够从失败中快速完全恢复；
» 考虑边缘计算场景独特性，安全功能可以部署在各类硬件资源受限的 IoT 设备中；
» 在关键的节点设备（例如边缘网关）实现网络与域的隔离，对安全攻击和风险范围进行控制，避免攻击由点到面扩展；
» 持续的安全检测和响应无缝嵌入到整个边缘计算架构中。

根据上述考量，边缘安全框架的设计需要在不同层级提供不同的安全特性，将边缘安全问题分解和细化，直观地体现边缘安全实施路径，便于联盟成员和供应商根据自己的业务类型参考实施，并验证安全框架的适用性，提出如下的边缘安全参考框架 1.0：

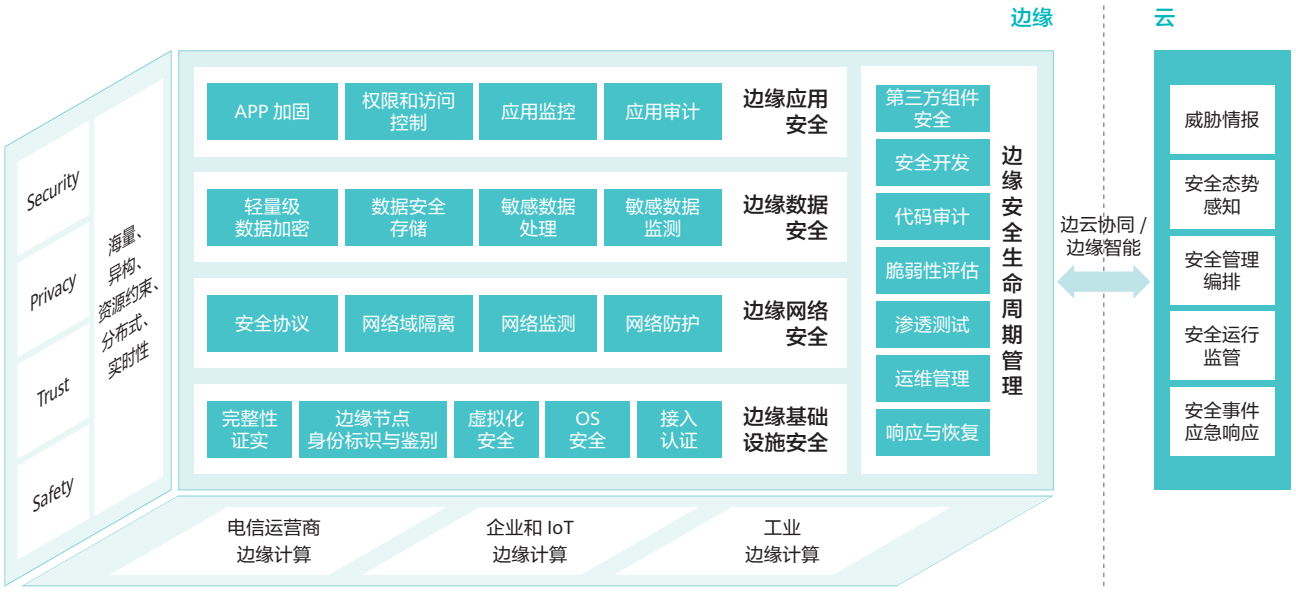


图 4 边缘安全参考框架 1.0

边缘安全参考框架的主要内容包括：

边缘安全参考框架覆盖了边缘安全类别、典型价值场景、边缘安全防护对象。针对不同层级的安全防护对象，提供相应的安全防护功能，进而保障边缘安全。另外，对于有高安全要求的边缘计算应用，还应考虑如何通过能力开放，将网络的安全能力以安全服务的方式提供给边缘计算 APP。

边缘安全防护对象覆盖边缘基础设施、边缘网络、边缘数据、边缘应用、边缘安全全生命周期管理以及边云协同安全“5+1”个层次；统筹考虑了信息安全（Security）、功能安全（Safety）、隐私（Privacy）、可信（Trust）四大安全类别以及需求特征；围绕工业边缘计算、企业与 IoT 边缘计算和电信运营商边缘计算三大典型的价值场景的特殊性，分析其安全需求，支撑典型价值场景下的安全防护能力建设。

对于具体的边缘计算应用场景的安全，还需根据应用的需求进行深入分析，并非所有的场景下都涉及到上述安全功能模块，结合具体的使用场景，边缘安全的防护功能需求会有所不同，即使是同一种安全防护能力，在与不同场景结合时其能力与内涵也会不尽相同。

3.1 多视图呈现

以 ISO/IEC/IEEE 42010:2011 架构定义国际标准为指导，将产业对边缘计算的关注点进行系统性的分析，并提出了解决措施和框架，通过安全功能视图和价值场景视图来展示边缘安全参考框架。

价值场景视图
阐述边缘安全的领域模型和关键概念。

安全功能视图
功能视图侧重于系统中的功能组件，它们之间的相互关系和结构，它们之间的接口和交互，以及系统与支持该系统活动的外部元素的关系和交互。系统和组件架构师，开发人员和集成商特别关注这些问题。

3.1.1 价值场景视图

根据市场价值细分，边缘计算典型的价值场景包括电信运营商边缘计算、企业和 IoT 边缘计算、工业边缘计算，其边缘安全的需求关注点各不相同。

1）电信运营商边缘计算

电信运营商边缘计算使能运营商可以在网络边缘分流业务，通过端到端整体方案的打包，从而为客户提供更低时延、更高带宽、更低成本的业务体验，快速响应用户请求并提升服务质量；同时通过网络能力开放，在自身孵化能力基础上对外合作，可以将移动网络的位置服务、带宽管

图 5 边缘计算典型价值场景

理等开放给上层应用，从而实现优化业务应用，开发新商业模式，进一步促进移动通信网络和业务的深度融合，提升网络的价值。借助电信运营商边缘计算，一方面提供丰富的网络管理的 API，便于全方位管控，增强客户体验；一方面运营商可以集成网络增值服务（如 vLB、vWoC 等）及创新类增值服务（如 VR/AR、游戏云、企业办公应用等），收益从管道转向软件与服务。

广域接入网络边缘计算以及多接入边缘计算是电信运营商边缘计算价值场景中主要的业务形态，多接入边缘计算（MEC）将密集型计算任务迁移到附近的网络边缘服务器，降低核心网和传输网的拥塞与负担，减缓网络带宽压力；广域接入网络边缘计算主要为企业客户提供灵活弹性的广域网络接入能力，帮助运营商实现对广域接入网络服务的端到端控制，支撑企业客户按需快速构建广域接入网络。

在电信运营商价值场景中，由于边缘计算平台和应用部署在通用服务器上，边缘计算的本地业务处理特性，使得数据在核心网之外终结，运营商的控制力减弱，攻击者可能通过边缘计算平台或应用攻击核心网，造成敏感数据泄露、未授权访问等安全问题。电信运营商边缘计算的核心部分涉及运营商网络的可靠覆盖、网络业务的本地分流等，其边缘安全除需要考虑边缘基础设施、网络域、平台和应用的安全以及管理之外，对于有高安全级别需求的移动边缘计算应用，运营商还应考虑如何通过能力开放，将网络的安全能力以安全服务的方式提供给移动边缘计算应用，保障自身安全性的同时，还能够满足大型企业数据本地化处理以及时延敏感性业务的部署需求以及安全防护，开发更多的商业模式，创造更多的网络价值。

2）企业和 IoT 边缘计算

全球联网设备数量高速增长，“万物互联”成为全球网络未来发展的重要方向。在企业与 IoT 边缘计算场景中，由于物联网节点分布广，数量多，应用环境复杂，计算和存储能力有限，无法应用常规的安全防护手段，使得物联网的安全性相对脆弱。随着物联网应用在工业、能源、电力、交通等国家战略性基础行业，一旦发生安全问题，将造成难以估量的损失。

与其他两类边缘计算相比，企业与 IoT 边缘计算在海量、异构和分布式等特点更加突出，IoT 终端资源受限的情况更加明确，软硬件系统的异构性更大；在应用方面，IoT 涉及到消防、安防、视频监控、市政基础设施等领域的应用，关系到关键基础设施和众多的用户隐私，更应该关注安全和隐私保护工作；另外，物联网领域的设备、软件、网络和集成商均较分散，没有形成行业垄断优势，标准化工作也相对比较滞后。

在边缘基础设施安全方面，IoT 分布在广泛的地理范围，难以做到集中的设备安全保护，很容易出现终端和设备被窃取、仿冒和非法接入的问题，因此更应当做好完整性证实、边缘节点识别、接入认证、OS 安全等工作。

从网络安全方面，IoT 设备分布较广，环境恶劣，完全部署专用的有线网络难以实现，更应该通过 VPN 等技术做好协议的接入安全，做好传输中的数据加密，采取有效措施防止数据在传输过程中被截获或者泄露；做好网络域隔离，防止受到攻击后的影响扩散。

由于物联网广泛应用于关键基础设施，涉及到众多的用户隐私数据，边缘数据安全应该在轻量级数据加密、数据安全存储以及敏感信息的处理和监测方面格外重视。

在边缘应用安全、边缘生命周期管理和边云协同方面，与其他类型基本相似。

3）工业边缘计算

工业边缘计算具有较强的行业特点，通过与工业设备及工业应用紧密结合，将工业领域的不同层级整合起来，贯穿工业生产单元的全工作流程，能够将传感器和控制设备产生的数据在本地进行处理和存储，使能工业系统的数字化，促进设备、工艺过程及工厂全价值链优化，加速 IT 和 OT 的融合。

在工业边缘计算价值场景中，自动化厂商依托于传统的现场优势，通过边缘计算增强本地计算能力，降低由云集中式计算带来的响应延迟，满足大规模复杂系统对工业设备优化、工业过程优化等子场景的计算能力和实时响应要求。同时结合工业云平台，为客户提供边云一体的解决方案，支撑自动化厂商的商业模式与业务模式创新（如从批量生产走向柔性生产，从产品价值走向产业 + 服务价值），在行业数字化过程中进一步获取产业价值。

随着工业边缘计算价值场景中边缘节点数量的激增，当前封闭的工业网络将会逐渐走向开放，致使工业控制安全、工业数据安全、平台安全（云端）问题突显。工业边缘计算安全的核心部分涉及工业控制、智能制造，它对安全的要求更高、波及面更广，工业边缘计算需要满足工业企业应用的高安全性、超可靠、低时延、大连接、个性化等要求，同时防范非法入侵和数据泄露。尤其原有的工业协议基本是专用的，未考虑信息安全威胁，工业设备多种多样、业务链长、模型复杂、需求繁多，信息技术与工业技术相互融合，采用优化 ICT 技术，性能和各项技术要求更高更复杂。

工业边缘计算安全将是覆盖工业系统设计、开发、实施、运维、结束等横向全生命周期，以及控制层、网络层、系统层、管理层等纵向运维，通过多维度安全技术的深度融合和集成设计，以保证工业边缘计算系统可用性为目标，综合运用信息安全、功能安全等技术手段和管理措施，实现工业边缘计算系统的安全稳定运行。

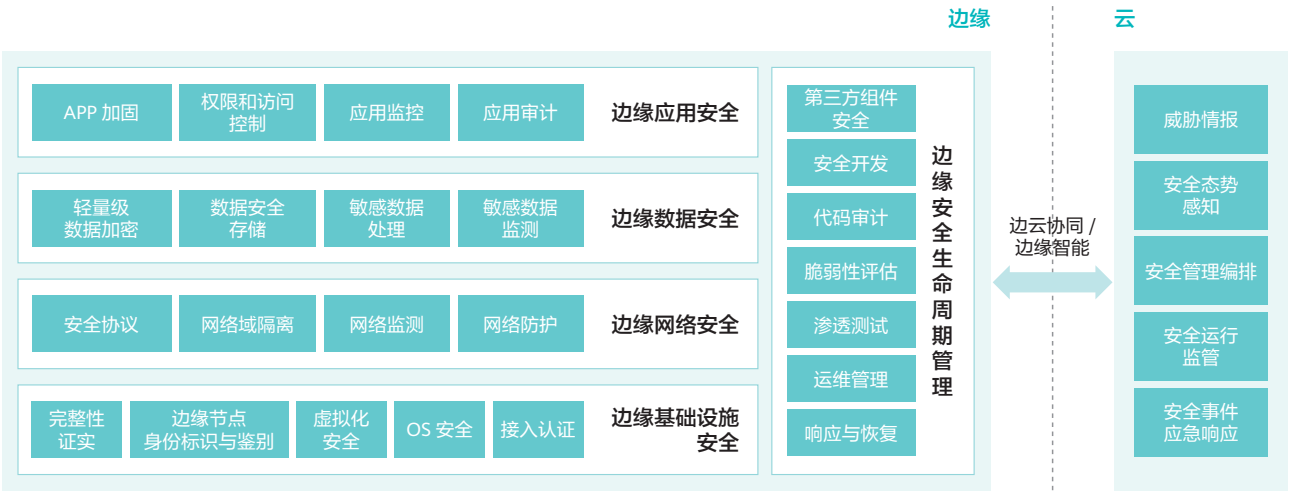


图 6 边缘安全功能视图

3.1.2 安全功能视图

为了帮助相关企业应对边缘安全面临的各种挑战，安全功能视图涵盖不同层级下的安全功能以及边云协同下的统一安全防护手段。

1）边缘基础设施安全

边缘基础设施为整个边缘计算节点提供软硬件基础，边缘基础设施安全是边缘计算的基本保障，需要保证边缘基础设施在启动、运行、操作等过程中的安全可信，建立边缘基础设施信任链条，信任链条连接到哪里，安全就能保护到那里。边缘基础设施安全涵盖从启动到运行整个过程中的设备安全、硬件安全、虚拟化安全和 OS 安全。

» **完整性校证实**

边缘计算完整性证实是指对边缘节点基础设施中的系统与应用进行完整性检查和验证，保障系统和应用的完整性，进而保证边缘节点运行在预期的状态，然而受限于边缘节点的计算资源和存储资源，低端异构的边缘设备往往无法执行复杂的计算，因此需要节点的安全证实服务能够突破对复杂设备类型管理能力的限制以及轻量级的可信链传递及度量方法，进行边缘节点启动和运行的度量以及验证结果的上传，保证边缘度量结果验证的时效性和准确性。

» **边缘节点的身份标识与鉴别**

边缘节点身份标识与鉴别是指标识、区分和鉴别每一个边缘节点的过程，是边缘节点管理、任务分配以及安全策略差异化管理的基础。在边缘计算场景中，边缘节点具有海量、异构和分布式等特点，大量差异性的边缘节点以及动态变化的网络结构可能会导致边缘节点的标识和识别反复进行，因此，能够自动化、透明化和轻量级的实现标识和识别工作是其核心能力。

» **虚拟化安全**

在边缘计算环境下，虚拟化安全是指基于虚拟化技术，实现对边缘网关、边缘控制器、边缘服务器的虚拟化隔离和安全增强。相较传统云服务器，这些边缘节点计算、存储等资源受限，低时延和确定性要求高，不支持硬件辅助虚拟化，面临虚拟化攻击窗口更加复杂广泛等问题。因此，需要提供低底噪、轻量级、不依赖硬件特性的虚拟化框架；需要基于虚拟化框架构建低时延、确定性的 OS 间安全隔离机制和 OS 内安全增强机制；需要增强 hypervisor 本身的安全保护，消减虚拟化攻击窗口。

» **OS 安全**

在边缘计算环境下，OS 安全是指各种应用程序底层依赖的操作系统的安全，如：边缘网关、边缘控制器、边缘服务器等边缘计算节点上的不同类型操作系统的安全。与

云服务器相比，这些边缘节点通常采用的是异构的、低端设备，存在计算、存储和网络资源受限、安全机制与云中心更新不同步、大多不支持额外的硬件安全特性（如 TPM、SGX enclave、TrustZone 等）等问题。因此，需要提供云边协同的 OS 恶意代码检测和防范机制、统一的开放端口和 API 安全、应用程序的强安全隔离、可信执行环境的支持等关键技术，在保证操作系统自身的完整性和可信性的基础之上，保证其上运行的各类应用程序和数据的机密性和完整性。

» **接入认证**

接入认证是指对接入到网络的终端、边缘计算节点进行身份识别，并根据事先确定的策略确定是否允许接入的过程。边缘计算架构中存在海量的异构终端，这些终端采用多样化的通信协议，且计算能力、架构都存在很大的差异性，连接状态也有可能发生变化。因此，如何实现对这些设备的有效管理，根据安全策略允许特定的设备接入网络、拒绝非法设备的接入，是维护边缘计算网络安全的基础和保证。

2）边缘网络安全

边缘网络安全是实现边缘计算与现有各种工业总线互联互通、满足所联接的物理对象的多样性及应用场景的多样性的必要条件。边缘计算环境下，由于边缘计算节点数量巨大、网络拓扑复杂，其攻击路径增加导致攻击者可以很容易的向边缘计算节点发送恶意数据包，发动拒绝服务攻击，影响边缘网络的可靠性和可信，边缘网络安全防护应建立纵深防御体系，从安全协议、网络域隔离、网络监测、网络防护等从内到外保障边缘网络安全。

» **安全协议**

安全协议是以密码学为基础的消息交换协议，其目的是在网络环境中提供各种安全服务，包括通过安全协议进行实体之间的认证、在实体之间安全地分配密钥或其它各种秘密、确认发送和接收的消息的非否认性等。边缘计算环境使用了多种通信协议来满足业务运行中的数据传输需求，既有和云端交换的北向接口协议又有和现场端交互的南向接口协议，这些通信协议的安全特性参差不齐，多数协议在设计之初就没有考虑安全性，缺乏认证、授权和加密机制，可能存在协议自身特点所造成的固有安全问题，协议演化到基于通用计算机、通用操作系统和 TCP/IP 后继承的安全问题，以及协议没能正确实现引起的安全问题等。因此，解决边缘计算安全协议的问题，一是需要保证协议自身安全性，从协议设计和实现分别展开，如对设计和实现逻辑一致性的问题，可通过漏洞挖掘评估其安全性；二是原有协议增加安全层，可以通过增加通信模块或者通信网关的方式，将原有协议再进行一次封装，通过 VPN、

SSL 等安全通道传输。但解决边缘计算协议的安全问题通常会带来新的兼容性问题，并且对已有国际标准和行业管理的通信协议进行修改也会遇到相应的阻力和困难。

» 网络域隔离

网络域隔离是指在边缘节点的不同虚拟机之间虚拟隔离资源，控制端的安全资源调配，实现不同业务场景下的安全隔离。在边缘计算环境中，边缘节点更倾向于使用轻量级容器技术，此时容器共享底层操作系统，使边缘节点之间隔离性更差、安全威胁更加严重。通常在边缘侧与云端之间通过隔离技术实现文件、数据的有效传输，防止由于云端安全风险所带来的威胁影响边缘侧业务的运行。因此，隔离技术需要通过对不同虚拟机之间通信的数据完整校验、数据的安全检查及建立无 TCP 连接的方式来实现不同业务通信单元之间有效的安全隔离。在虚拟化环境中隔离设备还可以接受控制端的调度，来提供隔离的能力。

» 网络监测

网络监测是指持续监控计算机网络是否存在缓慢或故障组件，并在故障、中断等情况下通知网络管理员。在安全领域，网络监测还应该具备发现网络攻击并及时通报给系统管理员的功能，但网络监测系统本身不具备自动阻断网络攻击和排除故障的功能。在边缘计算环境中，网络结构复杂，存在海量的设备和海量的连接，当这些设备同时进行通信时，可能会出现网络风暴。设备受到攻击后，也有可能会发起针对特定目标的分布式拒绝服务攻击 DDoS。因此，进行有效的网络监测是边缘计算网络安全的重要组成部分。通过监测网络流量，实时监测网络的传输内容，能够及时发现网络违规行为，防止边缘网络及设备受到网络攻击。

» 网络防护

网络防护是指对于明确的有害网络流量进行阻断、缓解和分流的措施。与网络监测不同的是，网络监测是通过流量分析发现可疑行为，并对网络管理员发出警报，而网络防护是根据流量分析和规则匹配，直接阻断有害流量，并生成日志。边缘侧安全需要考虑与云端对接的安全及与控制端对接的安全。与云端要建立起有效的加密通信认证机制，保证通信过程的可控。同时，要加强对边缘侧的安全监测，对边缘侧的流量进行检测，有效发现隐秘在流量中的攻击行为。此外，需要在边缘侧与控制端之间建立有效的安全隔离与防护机制，通过严格限制进入到控制网络的数据内容保证确定性的数据可以进入到控制网络中。

3）边缘数据安全

边缘数据安全保障数据在边缘节点存储以及在复杂异构的边缘网络环境中传输的安全性，同时根据业务需求随时被用户或系统查看和使用。在边缘计算环境下，由于边缘计算服务模式的复杂性、实时性，数据的多源异构性、感知性以及终端资源受限特性，传统环境下的数据安全和隐私保护机制不再适用于边缘设备产生的海量数据防护，亟待新的边缘数据安全治理理念，提供轻量级数据加密、数据安全存储、敏感数据处理和敏感数据监测等关键技术能力，保障数据的产生、采集、流转、存储、处理、使用、分享、销毁等环节的全生命周期安全，涵盖对数据完整性、保密性和可用性的考量。

» 轻量级数据加密

数据加密目前仍是对信息进行保护的一种最可靠的办法。对于边缘计算架构而言，分布在不同区域的边缘节点虽然具有一定的通信、存储和计算能力，但是在这些设备上直接采用传统的密码算法对数据进行加密具有极大的挑战性。因此，针对资源受限的边缘设备，需要提供经过定制或裁剪产生的密码解决方案。可考虑采用将边缘网关与商用保密机相结合的思路来实现集中式的轻量级加密，通过集成了多种成熟的密码算法的商用密码机提供快速、高效的密码运算服务，满足不同用户或者应用场景下的轻量级需求。

» 数据安全存储

边缘计算环境中的数据安全存储主要是指保证存储在边缘节点上的数据安全性，包括存储在边缘网关、边缘控制器、边缘服务器等节点上的静态数据的安全性。考虑到边缘计算系统的分布性、边缘节点的资源受限性、边缘数据的异构性等特点，安全措施需要考虑到数据存储方式（如分布式数据存储，兼顾安全和效率）、数据存储时的安全保护措施（如加密存储和存储数据访问控制，用来保证数据的保密性）、数据备份（用来保证数据的可用性）。

» 敏感数据处理

敏感数据处理是指对敏感数据进行识别、使用和保护的一系列活动。为保证边缘计算环境中数据的私密性，需要对大量敏感边缘数据进行有效的处理和管控。边缘敏感数据异构性强、存储位置分散、流动路径多样、业务应用关系复杂，为敏感数据处理带来一系列安全问题，这包括如何从复杂异构的关联数据集中识别出敏感的数据，如何在不影响边缘计算中应用业务的前提下对敏感数据进行脱敏混淆，如何在各边缘计算实体间安全地共享敏感数据等。通过对以上问题的解决，可以对边缘环境中的敏感数据的流动和分发使用进行统一的管控，在保证安全保密性的前提下最大程度地发挥数据的价值。

» 敏感数据监测

敏感数据监测是指对敏感数据处理和使用过程的审计跟踪，并在此基础上发现和处理存在的安全风险。边缘计算环境中敏感数据复杂多样，访问关系千变万化，虽然可通过识别、脱敏和共享管控对敏感数据进行管理，但为保证管控过程的有效性以及及时发现敏感数据传输和使用过程中的问题和风险，监测和审计能力不可或缺。考虑到敏感数据传输路径的复杂性，需要通过数据溯源技术对敏感边缘数据进行跟踪和记录，确保所有敏感数据流向都有迹可循，随时可根据需要进行查询。同时还需要在敏感数据溯源的基础上，对流动数据进行审计，包括对流动数据传输路径和访问行为进行综合分析并可视化展示，对异常行为进行识别并告警等。

4）边缘应用安全

边缘应用安全是满足第三方边缘应用开发及运行过程中的基本安全需求，同时防止恶意应用对边缘计算平台自身以及其他应用安全产生影响。由于边缘计算应用在不同的行业领域，为满足未来不同行业和领域的差异化需求，必须采用开放式的态度引入大量的第三方应用开发者，开发大量差异化应用，同时通过一系列措施保证其基本的安全。为了实现这一目标，边缘应用安全应在应用的开发、上线到运维的全生命周期，都提供 APP 加固、权限和访问控制、应用监控、应用审计等安全措施。

» APP 加固

APP 加固是指在边缘计算场景下，考虑性能和资源占用，对采用低级语言（比如，c 语言）编写的 APP 进行加固。

在边缘计算场景下，低级语言往往缺乏安全检查，存在大量内存漏洞，攻击者利用漏洞能够实现包括代码损坏攻击（code corruption attack）、控制流劫持攻击（Control-flow hijack attack），纯数据攻击（data-only attack）、信息泄露攻击（Information leak）等各种攻击手段。考虑到边缘计算场景轻量化的需求特征，安全加固（特别是数据保护）通常只能对敏感关键的模块实施。然而，考虑 App 逻辑和安全需求的复杂性、后续升级演进的需求，在 APP 中人工识别敏感关键部分易出错、效率低下。需要提供基于程序语言安全扩展和静态程序分析的、自动化的识别和安全加固机制。

» 权限和访问控制

权限与访问控制定义和管理用户的访问权限，通过某种控制方式明确的准许或限制用户访问系统资源或获取操作权限的能力及范围，控制用户对系统的功能使用和数据访问权限。由于边缘节点通常是海量异构、分布式松耦合、低时延以及高度动态性的低端设备，因此，需要提供轻量级的最小授权安全模型（如白名单技术），去中心化、分布式的多域访问控制策略，支持快速认证和动态授权的机制等关键技术，从而保证合法用户安全可靠的访问系统资源并获取相应的操作权限，同时限制非法用户的访问。

» 应用监控

应用监控指对应用的性能、流量、带宽占用、用户行为、用户来源渠道、用户客户端环境等进行实时监控、分析、报警。边缘应用通常部署在异构边缘节点上，需要与现场设备交互，功能单一、信息透明、安全性相对薄弱，容易被非法访问或恶意攻击并难以及时发现处理，因此需要应用监控来防范安全威胁。一般要在边缘节点对应用进行实时监控，并设立安全基线；对于违反安全规则的行为及时进行警告或者阻断，实现对边缘应用安全威胁的及时响应。边缘应用监控包括应用行为监控和应用资源占用监控，可以采用日志分析进行应用运行行为监控，通过在应用代码中埋点或安装监控工具进行性能监控。

» 应用审计

应用安全审计是指按照一定的安全策略，通过记录应用活动的信息，检查、审查和检验应用环境，从而发现应用漏洞、入侵行为的过程。边缘计算业务中网络环境更加复杂，需要应用安全审计来帮助安全人员审计应用程序的正确性、合法性和有效性，将妨碍应用运行的安全问题及时

报告给安全控制台。一般情况下，要定期采集各种设备和应用的安全日志并进行存储和分析，发现应用的违规、越权和异常行为，对违规操作预测报警并进行事后追溯。

5）边缘安全生命周期管理

边缘安全生命周期管理是将安全要素融入到边缘计算平台及应用生命周期的需求、开发、测试、运行等各个阶段，每一个阶段有一个或多个安全活动来缓解安全问题，由于边缘计算具有海量、异构和分布式的计算单元，边缘安全生命周期管理中应制定配套的安全制度和进行必要的安全培训，通过流程保障，不将缺陷带入下一个阶段，减少平台及应用的漏洞数量和严重程度。

» 第三方组件安全

第三方组件安全是指能够快速且全面的发现那些有问题的第三方组件，通过运行回归测试确保原有业务行为的正确性，及时避免第三方组件安全漏洞给应用带来安全风险。

边缘计算作为一个业务形态，从计算平台的供应商到应用 APP 开发生态所带来的安全风险都会威胁到边缘侧的安全。边缘计算整体环境中使用的大量第三方组件自身可能含有安全漏洞，给应用的整体安全性埋下隐患。第三方组件的风险控制能力随着供应商透明度降低而逐层降低，

任意环节存在设置恶意功能、泄露数据、中断关键产品或服务提供等行为都将破坏相关业务的连续性，带来不可控的安全风险。

针对第三方组件的风险需要建立供应商的审核机制，包含对供应上人员权限的管理、供应商提供设备和软件的安全性检验。制定代码开发规范，要求软件供应商的开发人员遵循相关的代码开发规范要求。制定有效的应急计划，包含影响性分析，辨识关键流程和组件及安全风险，确定优先顺序。提供应急的恢复目标，恢复优先级和度量指标建立第三方组件信息备份，保证备份信息的保密性、完整性和可用性，并定期验证信息系统备份的可用性。确保应急预案纳入到供应商的服务协议中。

» **安全开发**

安全开发是在应用软件开发的所有阶段引入安全和隐私的原则，将应用的安全缺陷降低到最小程度，通常指安全开发生命周期。在边缘计算环境下，存在不安全的通信协议、大量的异构节点、开放的接口和身份认证缺乏等情况，需要应用在设计开发过程中充分考虑安全性，减少漏洞的数量和严重性。一般安全开发过程包括需求阶段的安全需求分析和风险评估、设计阶段的攻击面分析与威胁建模、开发阶段的标准工具使用和静态分析（安全开发规范和代码审计）、测试验证阶段的异常缺陷评估和黑白盒测试、发布维护的最终安全审核。

» **代码审计**

代码审计（Code Audit）是一种以发现程序错误、安全漏洞和违反程序规范为目标的源代码分析。它是防御性编程范式的一部分。该范式的目标是在程序发布前减少错误。在边缘计算体系架构中，基于海量、异构和分布式架构构建的系统，应用在不同的领域，涉及不同行业和不同专业的众多开发者参与其中，开发者的安全基础参差不齐，难免会在开发中引入安全漏洞，影响最终系统的安全，有效的进行代码审计可以补齐短板，提高代码的整体安全水平。代码审计的核心价值是能在上线前发现错误、安全漏洞和违反编程规范的代码，从源头上减少程序的安全漏洞和安全问题，提高程序的内生安全性。

» **脆弱性评估**

脆弱性评估是指用于标识在开发过程中不同细化步骤引入的潜在缺陷的过程。在边缘计算环境下，评估的对象包括云服务器、云网关、边缘网关、边缘服务器、边缘控制器等一系列参与这一体系的设备。边缘节点通常是海量异构设备组成，可能导致诸如安全策略不兼容、不同的接口引入新的安全问题、硬件安全特性不支持等风险；边缘节点远离中心化的安全管理，容易遭受网络的劫持，在进行脆弱性评估时应该把网络传输的风险考虑进去。因此，边缘计算系统脆弱性评估的方法包括：一是需要能够对每种异构的系统进行评估，保证其自身的完整性和可信性；二是需要对开放的 API 和数据传输协议等网络体系进行评估，保证数据在传输过程中的机密性和完整性。

» **渗透测试**

渗透测试是从攻击者角度，对现有系统进行脆弱性发掘与利用，以达到系统风险评估的目的。在边缘计算环境下，测试对象包括云服务器、云网关、边缘网关、边缘服务器、边缘控制器等一系列参与这一体系的设备。渗透测试是脆弱性评估的一种方式。边缘设备具备 3 个特性：1 异构性，使其容易受到多种攻击；2 资源有限，使其无法装载重量级的保护机制；3 维护少、更新不及时，使其更强调每一个版本的安全和稳定。因此，边缘计算环境下，需要在渗透测试阶段制定具有保障可控性和完整性的测试方案，保证测试人员了解整个测试过程以及由此产生的结果，力求全面，同时边缘的异构分布式特性需要渗透测试合理利用分布式能力高效进行测试。

» 运维管理

运维管理是指帮助企业建立快速响应并适应企业业务环境及业务发展的 IT 运维模式，实现基于 ITIL 的流程框架、运维自动化。需要制定边缘安全运维管理策略，成立安全运维管理组织，制定安全运维管理规程，建设安全运维管理支撑体系，对边缘计算重要系统及设备等进行安全运行维护管理，能够及时发现并处置存在的脆弱性、入侵行为和异常行为。

» 响应与恢复

响应与恢复是指系统被入侵之后，做出反应和恢复的过程。系统的恢复过程中，通常需要解决两个问题：一是被入侵所造成的影响评估和系统的重建，二是恰当的外部措施的采取。其中外部措施的采取，又直接与评估和重建过程中所形成的结论相关。边缘计算采用网络、计算、存储、应用核心能力为一体的开放平台，就近提供最近端服务。其应用程序在边缘侧发起，需要产生更快的网络服务响应，满足行业在实时业务、应用智能、安全与隐私保护等方面的基本需求。因此，需要做好边缘安全应急响应准备工作，制定应急响应预案并演练，能够及时发现边缘安全事件并做出处置，阻止或减小事件影响。

6）边云协同安全

边缘安全除了考虑上述的防护对象外，还应考虑如何利用边云协同提高安全防护能力，通过结合流分析、大数据、AI 等技术深度挖掘数据价值，通过威胁情报、安全态势感知、安全管理编排、安全运行监管以及应急响应与恢复，实现边缘安全事情、事中、事后的及时防御和响应。

» 威胁情报

威胁情报是利用大数据、分布式技术等来尽可能的获取威胁、漏洞、行为以及特征等相关的知识信息，通过融合分析让用户对网络安全威胁根据可见性来进行更深入的了解和更有效的预防应对，从而有效地减少用户已经发生或者可能发生的损失。在边缘计算环境下，通过数据协同、服务协同、智能协同等边云协同核心能力，在云端构建细颗粒度的威胁情报库，支撑对各类特征库告警、网络攻击、安全事件、黑客画像分析、威胁情报、受攻击边缘节点分析等能力，实现边缘计算环境下威胁情报的搜集、处理和使用，让威胁与保护对象清晰可见。

» **安全态势感知**

态势感知是指在一定时间和空间内观察并理解系统中的元素及其意义，形成对系统整体状况的把握，并能预测系统近期未来的状态的一种方法。在边缘计算环境下，通过边缘与云的数据协同、服务协同，支持在云端对关键重要边缘节点进行持续监控，将实时态势感知无缝嵌入到整个边缘计算架构中，实现对边缘计算网络的持续检测与响应。

» **安全管理编排**

安全管理编排是以自动化的方式综合运用经编排的不同技术中的元素，帮助企业和组织解决边缘计算环境下安全运维自动化问题，驱动安全事件妥善解决，以期合理地分配安全资源，实现安全服务自动化、高效化和智能化。在边缘计算环境下，借助边云管理协同的能力和内涵，通过云端定义、排序和驱动最小化事件响应过程中重复性的任务，并自动化的编排在边缘节点进行部署和运行，实现自动化和自适应安全策略编排，并有效提高时间响应速度，降低用户的平均响应时间。

» **安全运行监管**

安全运行监管通过构建一个信息安全团队持续监控和分析边缘计算环境的安全状态，安全运行监管是一个持续的迭代过程，这样的理念也体现出了相对的、动态的安全观，而认为所有的技术手段和方法都是解决某一阶段问题的具体手段，持续的迭代优化才能实现安全目标。在边缘计算的场景下，分布式、海量、异构设备通过多样化通信协议连接起来，系统面临全新的安全威胁，将会面临大量的未公开漏洞和未知威胁，简单通过一系列安全防护措施就能保证系统的整体安全是不现实的。必须通过建立持续运行监管的安全理念，构建安全运行监管团队，健全安全运行监管流程，汇聚安全监测和防护信息，打通安全信息收集、关联分析和事件响应的流程，才能有效保障边缘计算系统的安全。

» **安全事件应急响应**

应急响应与恢复通常是指一个组织为了应对各种意外事件的发生所做的准备以及在事件发生后所采取一系列措施恢复原来的状态。在边缘计算场景下，当边缘计算系统发生网络与信息安全事件时，首先应区分事件性质，然后再根据不同情况分别进行处置。此时的应急响应与恢复工作包括准备、确认、遏制、根除、恢复、跟踪。因此，需要不断加强边缘网络安全监测，及时收集、分析、研判监测信息，主动发现网络与信息安全事件倾向或苗头，及早采取有效措施加以防范，使各种安全隐患消除在萌芽状态。

3.2 边缘安全十大关键技术

针对边缘基础设施、网络、数据、应用、全生命周期管理、边云协同等安全功能需求与能力，需要相应的安全技术的支持。

边缘计算节点接入与跨域认证

针对边缘计算节点海量、跨域接入、计算资源有限等特点，面向设备伪造、设备劫持等安全问题，突破边缘节点接入身份信任机制、多信任域间交叉认证、设备多物性特征提取等技术难点，实现海量边缘计算节点的基于边云、边边交互的接入与跨域认证。

边缘计算节点可信安全防护

面向边缘设备与数据可信性不确定、数据容易失效、出错等安全问题，突破基于软 / 硬结合的高实时可信计算、设备安全启动与运行、可信度量等技术难点，实现对设备固件、操作系统、虚拟机操作系统等启动过程、运行过程的完整性证实、数据传输、存储与处理的可信验证等。

边缘计算拓扑发现

针对边缘计算节点网络异构、设备海量、分布式部署等特点，面向边缘计算节点大规模 DDoS 攻击、跳板攻击、利用节点形成僵尸网络等安全问题，突破边缘计算在网节点拓扑实时感知、全网跨域发现、多方资源关联映射等技术难点，形成边缘计算的网络拓扑绘制、威胁关联分析、在网节点资产与漏洞发现、风险预警等能力，实现边缘计算节点拓扑的全息绘制。

边缘计算设备指纹识别

针对边缘计算设备种类多样化、设备更新迭代速度快、相同品牌或型号设备可能存在相同漏洞等特点，突破边缘计算设备主动探测、被动探测、资产智能关联等技术难点，形成对边缘设备 IP 地址、MAC 地址、设备类型、设备型号、设备厂商、系统类型等信息的组合设备指纹识别等能力，实现边缘计算设备安全分布态势图的构建，帮助管理员加固设备防护，加强资产管理，并帮助后续制定防护策略，为安全防护方案提供参考。

边缘计算虚拟化与操作系统安全防护

针对边缘计算边云协同、虚拟化与操作系统代码量大、攻击面广等特点，面向虚拟机逃逸、跨虚拟机逃逸、镜像篡改等安全风险，突破 Hypervisor 加固、操作系统隔离、操作系统安全增强、虚拟机监控等技术难点，形成边缘计算虚拟化与操作系统强隔离、完整性检测等能力，实现边缘计算虚拟化与操作系统的全方位安全防护能力。

边缘计算恶意代码检测与防范

针对边缘计算节点安全防护机制弱、计算资源有限等特点，面向边缘节点上可能运行不安全的定制操作系统、调用不安全第三方软件或组件等安全风险，突破云边协同的自动化操作系统安全策略配置、自动化的远程代码升级和更新、自动化的入侵检测等技术难点，形成云边协同的操作系统代码完整性验证以及操作系统代码卸载、启动和运行时恶意代码检测与防范等能力，实现边缘计算全生命周期的恶意代码检测与防范。

边缘计算漏洞挖掘

针对边缘计算设备漏洞挖掘难度大、系统漏洞影响广泛等特点，面向等安全问题，突破边缘设备仿真模拟执行、设备固件代码逆向、协议逆向、二进制分析等技术难点，形成基于模糊测试、符号执行、污点传播等技术的边缘计算设备与系统漏洞挖掘能力，实现边缘计算设备与系统漏洞的自动化发现。

边缘计算敏感数据监测

针对边缘计算数据的敏感性强、重要程度高等特点，面向数据产生、流转、存储、使用、处理、销毁等各个环节的数据安全风险，突破敏感数据溯源、数据标签、数据水印等技术难点，形成对敏感数据的追踪溯源、敏感数据的流动审计、敏感数据的访问告警等能力，实现边缘计算敏感数据的实时监测。

边缘计算数据隐私保护

针对边缘计算数据脱敏防护薄弱、获取数据敏感程度高、应用场景具有强隐私性等特点，面向边缘计算隐私数据泄露、篡改等安全风险，突破边缘计算轻量级加密、隐私保护数据聚合、基于差分隐私的数据保护等技术难点，实现边缘计算设备共享数据、采集数据、位置隐私数据等数据的隐私保护。

边缘计算安全通信协议

针对边缘计算协议种类多样、协议脆弱性广泛等特点，面向协议漏洞易被利用、通信链路伪造等安全风险，突破边缘计算协议安全测试、协议安全开发、协议形式化建模与证明等技术难点，实现边缘计算协议的安全通信。

04

典型场景下的边缘安全案例

4.1 智能制造领域边云协同场景下的典型安全解决方案

某电子制造企业为适应多品种、小批量、高效率的生产需求，将生产车间进行智能化改造，通过各系统间信息集成，达到了敏捷、透明、可视化生产，建设成为智能制造示范标杆。但随着各系统间的深度互联，信息安全风险也不断增大，在防护体系尚未完善的情况下，遇到了一系列问题，对生产制造的连续运行造成影响。

安全问题和需求：

电子车间同时存在多条生产线，设备数量众多，类型多样，包括生产 PC、PLC、运动控制器 MC、HMI、机械臂、AGV 小车、自动化仓库、工业相机等。设备间存在有线通信和无线通信方式，通信关系复杂，使用多种通信协议且多为非安全协议。不同产线间没有采取网络隔离措施，各设备处于全联通状态，缺少访问控制措施。若部分设备存在漏洞被攻陷，就会对其它设备造成影响。

电子车间网络和边缘层网络（MES 系统、边缘网关）之间由于业务需要存在通信连接，但未采取隔离措施或者访问控制规则，同时 MES 网络和办公网之间也存在连接。如果存在病毒或受到其它攻击，很容易蔓延到电子车间。

电子车间各主机采用较为老旧的操作系统，且未进行及时的补丁更新，未采用主机加固措施，致使部分主机受到攻击、感染病毒，出现蓝屏死机、向车间内其它设备发送攻击性报文等现象。这种情况若不在重装系统、有效查杀的基础上进行系统加固，很难彻底解决。

电子车间未部署监测审计设备和安全管理设备，缺少对生产网络的实时安全监控，无法及时发现系统中存在的异常流量和异常行为，因此也无法及时感知安全威胁并进行告警。

解决方案：

基于以上情况，需要对电子生产车间的信息安全问题形成整体解决方案，通过建立综合性防护体系全面彻底地解决问题。

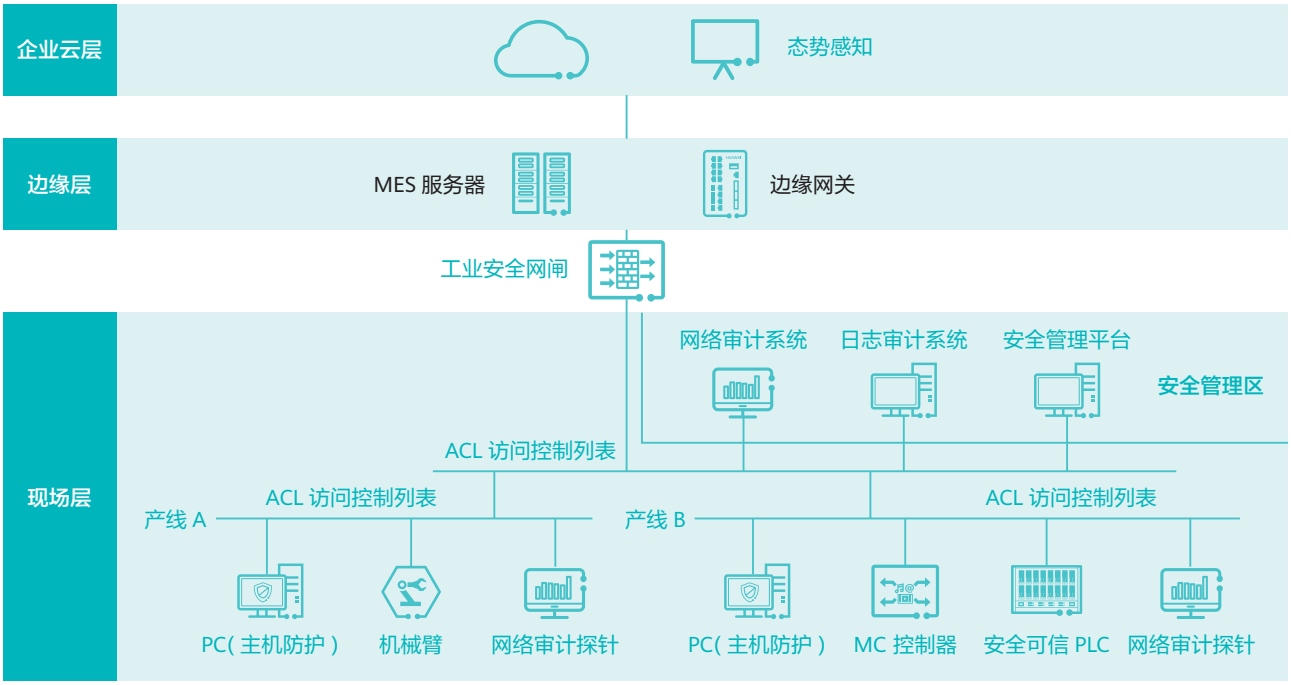


图 7 智能制造领域边云协同安全方案

对现场层网络拓扑进行改造，进行网络区域划分，采用 VLAN 方式对不同生产线的设备进行隔离。通过可设置 ACL 规则的可管理型交换机，通过访问控制规则屏蔽非必要通信，对关键设备进行防护。

电子车间网络和边缘层网络（MES 系统、边缘网关）之间采用工业网闸进行隔离，防止边缘层的网络安全问题蔓延到电子车间。

对电子车间的主机进行系统重装或病毒查杀，在此基础上安装主机防护软件。主机防护软件采用以可信计算技术为基础的工业白名单机制，构建自主防御体系，实现对终端运行环境的可信认证、可信度量和可信监控，抵御未知病毒、木马、恶意代码的攻击。

在满足控制要求的工段部署安全可信 PLC，替换原来不具备安全能力的普通 PLC。安全可信 PLC 融合嵌入式可信计算、数字证书体系、深度协议控制、虚拟化隔离等先进技术，采用双体系嵌入式架构，以可信加密芯片为基础，实现了从可信根到上层应用的完整性度量，包括静态度量和动态度量，具备对内核、应用、数据、工业业务行为的度量控制和检测审计能力。

部署综合审计产品，采集网络流量和各种设备的日志信息并进行审计，及时发现系统运行过程中的异常情况并进行告警。

部署安全管理平台，对车间安全设备、主机防护软件、安全可信 PLC 等进行统一管理，及时了解现场安全情况，并根据需要进行安全策略下发。

在企业云端部署安全态势感知平台，通过边缘层采集电子车间网络环境中各主机、设备的安全相关数据并进行集中分析，从而实现云端和边缘侧的边云安全协同。

核心价值：

本方案为智能制造领域边云协同场景下的典型安全解决方案，可以有效地解决电子制造公司的边缘层安全问题，并和云端进行安全协同。方案采用安全可信控制器系统、可信工业白名单等内生安全技术，结合传统防护手段，建立主动安全防御体系，为工业场景的边缘安全提供示范参考。

4.2 泛终端安全准入典型案例

终端网络安全准入系统主要解决边缘基础设施安全中的接入认证问题，可实现终端层面的访问控制，核心区域的访问控制，接入层边界的访问控制，满足不同网络场景下轻、中、高强度的准入控制需求。同时适应复杂网络环境下的终端接入控制，确保只有合法用户才能接入网络，保障业务的稳定运行，实现实名制认证、统一管理要求，从而使接入认证管理变得安全、透明、可控。

安全问题和需求：

随着信息技术的快速发展，各种网络应用的日益增多，病毒、木马、蠕虫以及黑客等等不断威胁并入侵企业内部网络资源，其终端接入主要面临以下安全挑战：

» 网络出口处部署了大量的网络安全设备，如：防火墙、IPS、防病毒服务器等安全设备，出口严防，但内部终端接入还是开放、透明的网络，如何防止从内部的非法接入访问
» 核心业务的访问安全，如核心数据、重要业务系统（如 ERP、OA）访问等安全问题
» 大量终端分散在企业内，并通过信息口接入网络，但如何保证终端合法及入网安全基线是否合规
» 智能手持设备、无线设备的接入安全问题
» 企业存在大量的哑终端设备，如：网络打印机、视频会议系统、IP 网络电话等设备，如何保证接入合法及接入的有效控制
» 如何定位追踪终端接入网络行为并进行有效的安全分析和审计

以上安全挑战使得企业网络的安全边界迅速缩小，开放的内部网络访问严重影响企业基础设施的稳定运行和数据安全，因此需要构建新一代的内部终端准入安全防御体系——终端网络安全准入系统（NAC）。

解决方案

若该企业终端有以下两种情况，一是集中在一个区域管理范围或总部核心交换设备通过光纤、专线等大带宽网络连接二级单位的企业，二是光纤和专线数据传输带宽比较大，能够保障服务器和终端的认证数据通讯的企业，这两种情况可以在总部核心交换机上集中部署 NAC 引擎设备，并做双机热备，如果用户认证终端规模比较大，这种部署方式需应对大量的数据通讯，这就要求服务器的性能好，数据处理能力强，保证设备服务的持续和稳定运行，需选配终端强制合规网络安全准入系统（NAC）进行安全防护。

该方案采用集中式部署的优点是实施部署简单，成本低，终端“一体化”控制台统一管理，但缺点是风险性比较大，当发生故障时影响面会比较广，对于准入控制来说此种部署方式适用于规模比较小，相对比较独立的网络环境部署。如：分支机构比较多、连接方式是窄带宽的情况下尽量采用分布式部署，准入设备下移，减小风险隐患。

终端强制合规网络安全准入系统（NAC）硬件设备采用旁路部署，并做双机热备、可减少对企业现有网络环境的改动，避免造成单点故障，如图 7 所示，对于那些对网络连续性要求极高的企业，其优点是它对客户网络环境和网络性能无任何影响，不会引入新的故障点，方便统一管理。

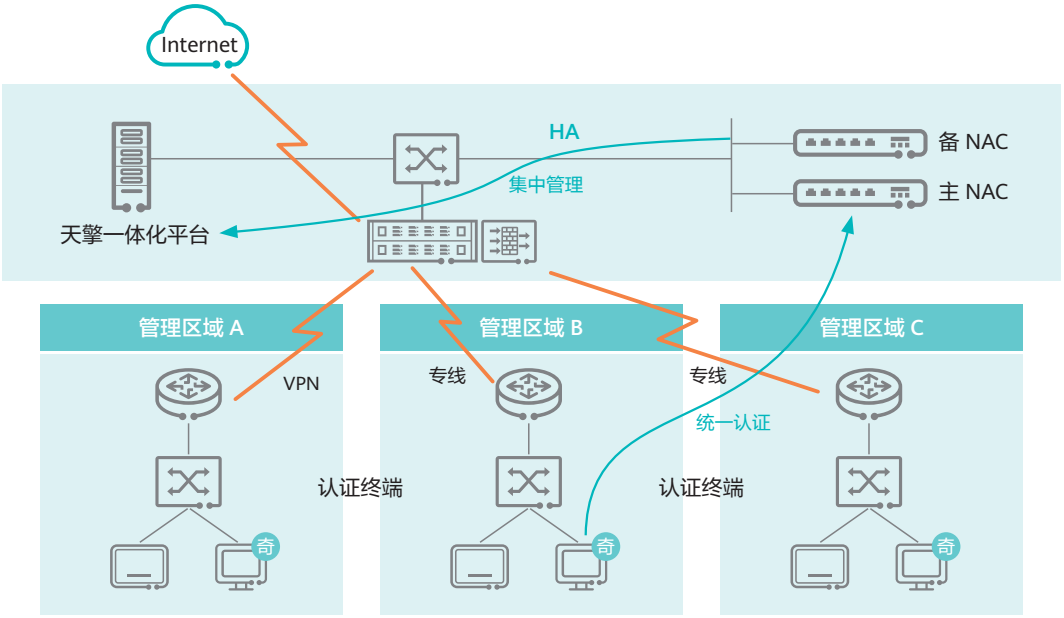


图 8 泛终端准入系统部署方案

核心价值

集中管理：基于终端准入安全防御体系集中管理与监测，分权分域管理，实名制统一认证，实现分布式部署、集中管理的特点，满足大型网络环境下的部署要求。

灵活的控制力度：具备多种准入控制方式，可实现核心区域的访问控制，终端层面的访问控制，接入层边界的访问控制，满足不同网络环境下轻、中、高强度的准入控制需求。

协同联动：实时监测终端是否安装防护点，快速引导安装，安装成功后执行合规检查，保障入网终端始终处于合规、可控范围内，实时上报安全动态及入网数据进行风险分析。

统一实名制认证：支持 AD、LDAP、Email、Http 多种第三方服务器联动认证，确保实名制统一认证管理，使终端接入管理变得安全、透明、可控，满足信息安全管理要求。

保障核心业务安全：保护核心服务器的访问安全，强制规范终端入网流程，确定身份和终端安全合规后才可访问，满足企业入网的强制合规管理要求。

网络边界准入控制：支持端口级的强准入控制，多种绑定认证方式，满足不同强度需求，严格禁止非法接入，保障边界接入安全。

全面隔离“危险”终端入网：支持多种合规检查策略，确保入网访问的终端是安全可信的，入网检查、隔离修复、访问控制，一站式引导修复入网流程。

4.3 自动驾驶边缘安全案例

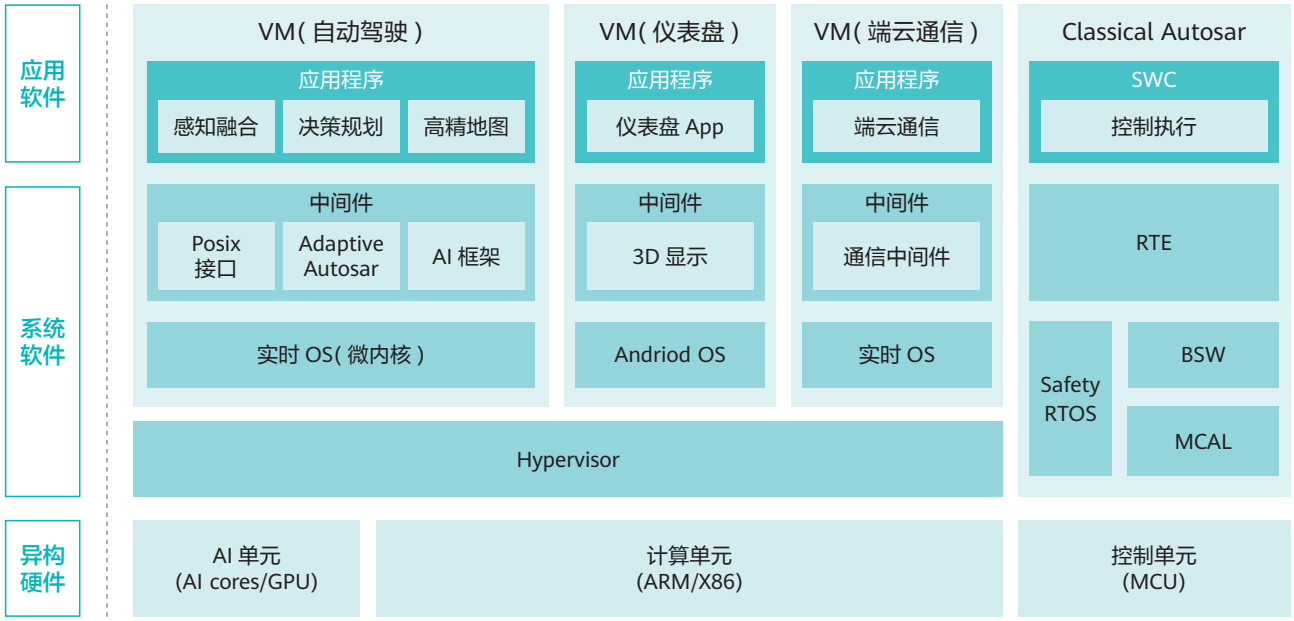


图 9 自动驾驶软硬件

自动驾驶软硬件主要包括异构硬件平台，系统软件和应用软件。异构硬件平台由计算单元、AI 单元和控制单元组成。计算单元通常采用多核 ARM/X86 芯片，运行自动驾驶 (感知融合、决策规划) 、仪表盘、端云通信相关的系统软件和应用软件。控制单元加载 Classic AUTOSAR 系统软件，运行车辆控制执行相关的应用软件，实现车辆动力学横纵向控制。AI 单元采用 GPU、AI 芯片、FPGA 等并行计算架构芯片，依赖系统软件进行资源分配和调度，完成图像、激光雷达数据的 AI 处理。

安全问题和需求：

从传统汽车封闭场景到自动驾驶开放场景，自动驾驶软件逻辑复杂，代码量大，安全漏洞难以避免，一旦被攻陷，很可能造成车毁人亡甚至更加严峻的公共安全问题。同时也面临广泛的、新型的攻击窗口，主要包括：

» 物理攻击窗口：通过 OBD、USB 等物理接口，实现接触型攻击；
» 近程攻击窗口：通过 NFC、RF、WIFI、蓝牙等近距离通信方式实现非接触型攻击；
» 远程攻击窗口：通过 3G/4G/5G、GPS 等远距离通信方式实现非接触型攻击。

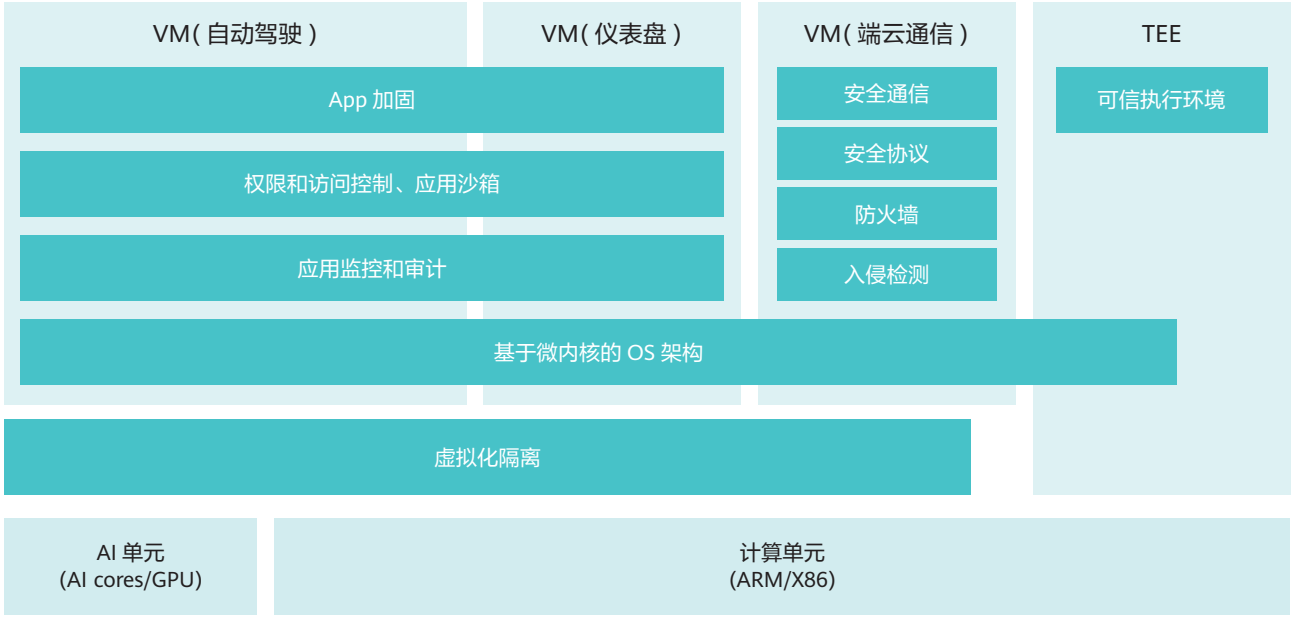


图 10 自动驾驶平台安全防护方案

解决方案：

针对上述安全问题和需求，自动驾驶安全解决方案包括：

» 构建基于硬件可信根（比如 HSM）的安全启动机制，保证从 HSM 到 hypervisor、hypervisor 到多 OS 的安全信任链。

» 基于虚拟化隔离，将不同安全级别的业务部署在不同的虚拟机中。其中，自动驾驶业务安全级别高、相对比较封闭，应部署在独立的虚拟机中；端云通信业务和仪表盘面临广泛的远程攻击窗口和近程攻击窗口，也应分别部署在独立的虚拟机中，确保即使这些虚拟机被攻陷，也难以影响高安全级别的自动驾驶业务。

» 操作系统采用基于微内核的安全架构，保证内核攻击窗口和可信基最小化。

» 基于 Trustzone 构建安全运行环境，保证敏感逻辑（AI 模型、加解密计算等）和敏感数据（密钥、身份信息）的完整性和私密性。

» 构建基于容器的应用沙箱，同时对应用行为（进程通信、文件访问、网络行为等）进行监控和日志审计。

» 对应用程序进行安全加固，利用程序分析和编译器插装等手段，保护应用代码完整性和私密性、控制流完整性、关键安全敏感数据的保护。

» 对于端云通信 VM，进一步构建网络安全通信和安全监控机制，通过融合身份认证、安全通信、防火墙、入侵检测等技术，提升主动防御能力。

核心价值：

本方案为自动驾驶场景下的典型的边缘安全解决方案，可以有效解决自动驾驶软硬件平台面临的 Trust、Privacy 等安全问题，并通过虚拟化资源隔离等关键技术，支撑高安全级别、相对封闭的自动驾驶业务的可信运行，同时也利用 APP 加固等技术手段，保护应用代码完整性和私密性、控制流完整性、关键安全敏感数据的保护。

4.4 C2M- 家具定制行业 - 边缘安全解决方案

C2M（Customer-to-Manufacturer 用户直连制造）是一种新型的工业互联网电子商务的商业模式。C2M 模式基于互联网、大数据、人工智能，以及通过生产线的自动化、定制化、节能化、柔性化，运用庞大的计算机系统随时进行数据交换，按照客户的产品订单要求，设定供应商和生产工序，最终生产出个性化产品的工业化定制模式。

家具定制行业，客户需求繁多，每个客户都有自己的需求，这要求家具定制工厂具备单品的快速换产能力，所以需要在每个车间或者产线部署边缘计算节点，在边缘侧实现生产数据的快速处理、储存和传输。为了预防和减少家具定制工厂在生产过程中的安全风险，保障企业的财产安全，需要在边缘侧进行相应的安全防护。

安全问题和需求：

» 边缘设备缺乏可信安全防护，一旦被黑客黑入，边缘设备面临恶意代码的植入或者恶意系统更新的风险；
» 边缘设备缺乏安全隔离机制，生产数据和敏感数据暴露在系统中，容易被黑客窃取；
» 边缘设备缺乏网络访问控制与实时异常行为检测，出现问题无法快速定位以及有效的安全防护；
» 边缘设备缺乏强有力的安全身份认证和管理，设备可以被伪造，一方面山寨给设备厂商带来财产损失，另一方面，恶意的设备也可以伪造成合法设备，给工厂安全生产带来风险；
» 边缘设备未建立安全通信，面临窃听，匿名攻击，接入点伪装，中间人攻击，重放攻击等网络攻击问题；
» 边缘设备缺乏硬件调试口和通信接口管控，甚至普通工人都可以通过 U 盘拷取相关数据和资料。

解决方案：

家具定制工厂网络拓扑结构包括办公区，生产区，MES 等。边缘网关管理一条产线或者一个车间，连接多个设备，边缘网关管理机床设备的接入，生产文件的下发，设备信息的上报，生产数据的安全传输、存储和处理，如图所示。

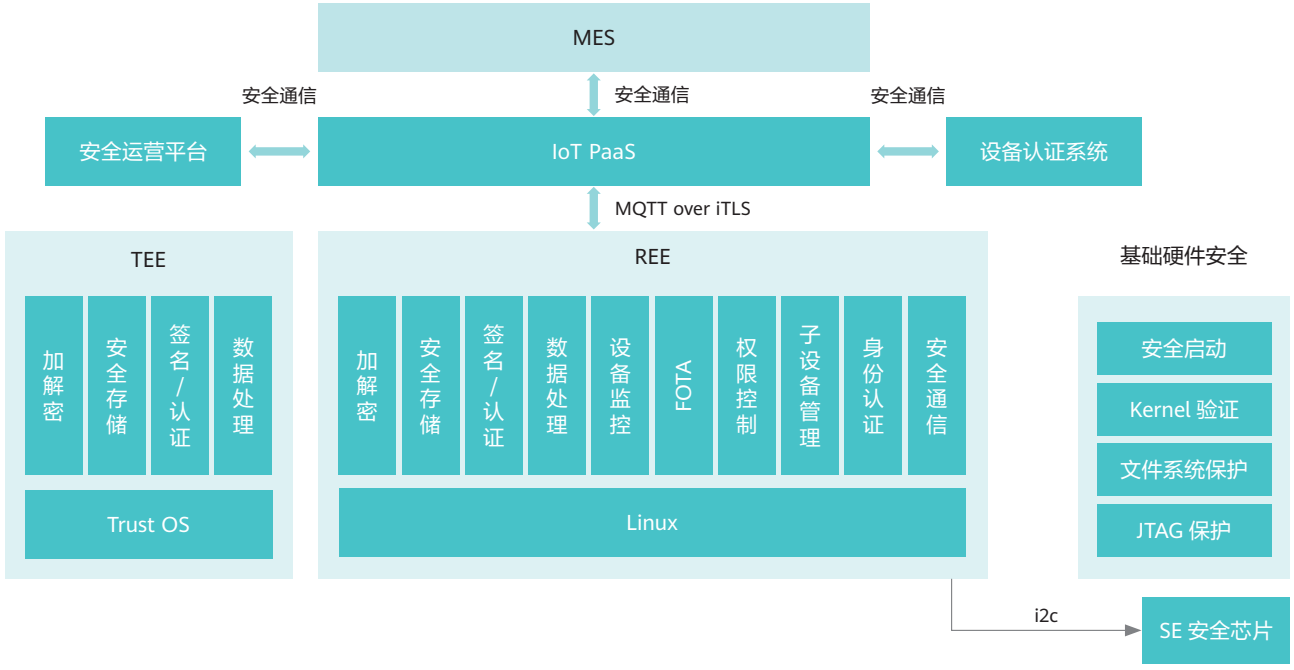


图 11 C2M 家具定制行业边缘安全软硬件框架

» 利用 Trustzone 进行硬件资源的隔离，将边缘计算系统划分成 secure world（安全世界）和 normal world（非安全世界），将生产过程中的敏感数据的操作放在 secure world 处理，保护定制家具生产过程中的敏感数据包的明文和相应的加密密钥的安全。
» 利用芯片硬件机制建立安全启动和信任链保证整个软件系统的安全可信，从 BootRom 开始逐级建立可靠的安全校验方案。
» 搭建安全管理运营平台，在边缘设备发布上线之前进行安全检测，基于行为生成安全基线和防护策略，识别和阻断基线范围外的异常行为（包括网络行为，进程行为，系统对象），提升风险识别和处置能力，并检测设备存在的安全漏洞，提供相应的修复措施和建议，防止威胁侵入，保障边缘网络访问控制与实时异常行为检测。
» 利用 Secure Element 安全芯片作为 ID2 的安全载体，为每个边缘设备提供唯一的标识信息，防止设备被篡改或仿冒，支撑设备身份信息的存储和认证，同时，利用安全芯片建立轻量级的安全通信，在保障安全通信的同时大幅减少 IoT 设备的资源消耗。

核心价值：

针对 C2M 定制家具行业，该解决方案解决了边缘网关的身份安全识别和接入，生产数据的安全传输、存储和处理，系统启动和运行的安全，异常行为的检测和监控等安全需求，有效的支撑了家具定制生产过程中边缘侧数据的快速处理、储存和传输，预防和减少了家具定制工厂在生产过程中的安全风险，保障企业的财产安全。

附录 1

术语表

序号	中文名称	英文名称	定义
1	云计算	Cloud Computing	云计算通常简称为“云”。通过互联网，“按使用量付费” 的方式提供随需应变的计算资源（从应用到数据中心）。其部署方式包括公有云、私有云和混合云。
2	边缘计算	Edge Computing	在靠近物或数据源头的网络边缘侧，融合联接、计算、存储、应用核心能力的开放平台，就近提供边缘智能服务，满足行业数字化在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求。
3	智能资产	Smart Asset	通过融合网络、计算、存储等 ICT 能力，具有自主化和协作化能力的资产（物）。
4	智能网关	Smart Gateway	通过网络联接、协议转换等功能联接物理和数字世界，提供轻量化的联接管理、实时数据分析及应用管理功能的网关。
5	智能系统	Smart System	基于多个分布式智能网关、服务器的协同构成智能系统，提供弹性扩展的网络、计算、存储能力。
6	智能服务	Smart Service	基于模型驱动的统一服务框架，面向系统运维人员、业务决策者、系统集成商、应用开发人员等多种角色，提供开发服务框架和部署运营服务框架。
7	异构计算	Heterogeneous Computing	是将不同类型指令集和不同体系架构的计算单元协同起来的新计算架构，即异构计算，以充分发挥各种计算单元的优势，实现性能、成本、功耗、可移植性等方面的均衡。
8	信息安全	Security	信息在网络传输中的保密性和完整性、控制访问受限网域与敏感信息以及在公共网络如因特网上使用隐秘通讯
9	功能安全	Safety	当任一随机故障、系统故障或共因失效都不会导致安全系统的故障，从而引起人员的伤害或死亡、环境的破坏、设备财产的损失，也就是装置或控制系统的安全功能无论在正常情况或者有故障存在的情况下都应该保证正确实施。

附录1：术语表

序号	中文名称	英文名称	定义
10	可信	Trust	围绕着“保证”和信心，即人、数据、实体、信息或流程将以预期的方式运行或表现。信任可能是人对人的，机器对机器的，人对机器的或者机器对人的。在更深的层次上，信任可能被视为朝着安全或隐私目标的一系列进展。
11	隐私	Privacy	隐私涉及表达或遵守各种法律和非法律规范。
12	TrustZone	ARM TrustZone	系统范围的安全方法，针对高性能计算平台上的大量应用，包括安全支付、数字版权管理 (DRM)、企业服务和基于 Web 的服务。
13	C 操作系统启动代码	BootRom	操作系统集成的启动代码，BootRom 是由 VxWorks 提供的一个 bootloader 程序，通过它可以和 Tornado 集成的一些工具进行 VxWorks 内核的下载和调试工作。
14	经典 AutoSAR	Classic AUTOSAR	是面向通信协议栈所有以太网层级提供支持的版本。包括诊断日志和跟踪功能（在系统服务层中），并更新了配置模式，提供系统级、ECU 级和模块级配置描述，AUTOSAR（经典平台）4.0 可用于汽车和工业应用，但不得用于高度危险的应用
15	低速短距离传输的无线网上协议	ZigBee	低速、低耗电、低成本、支持大量网上节点、支持多种网上拓扑、低复杂度、快速、可靠、安全的低速短距离传输无线网上协议

附录 2

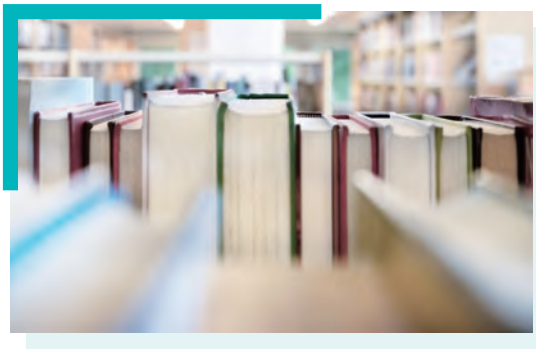
缩略语表

序号	中文名称	英文名称	中文名称
1	AI	Artificial Intelligence	人工智能
2	AC	Agile Controller	敏捷控制器
3	ACL	Access Control List	访问控制列表
4	AD	Altium Designer	AD 域认证
5	AGV	Automated Guided Vehicle	自动导引运输车
6	AII	Alliance of Industrial Internet	工业互联网产业联盟
7	API	Application Programming Interface	应用程序接口
8	APT	Advanced Persistent Threat	高级持续性威胁
9	APP	Application	应用程序
10	AR	Augmented Reality	增强现实
11	ARM	Advanced RISC Machines	英国 ARM 公司
12	AWS	Amazon Web Services	亚马逊公司旗下云计算服务平台
13	ASIC	Application Specific Integrated Circuit	应用集成电路
14	CDN	Content Delivery Network	内容分发网络
15	C2M	Customer-to-Manufacturer	用户直连制造
16	DC	Data Center	数据中心

附录2：缩略语表

序号	中文名称	英文名称	中文名称
17	DDoS	Distributed Denial of Service	分布式拒绝服务
18	ECC	Edge Computing Consortium	边缘计算产业联盟
19	ECN	Edge Computing Node	边缘计算节点
20	EC-IaaS	Edge Computing Infrastructure as a Service	边缘基础设施即服务
21	EC-PaaS	Edge Computing Platform as a Service	边缘平台即服务
22	EC-SaaS	Edge Computing Software as a Service	边缘软件即服务
23	FPGA	Field – Programmable Gate Array	现场可编程门阵列
24	GPU	Graphics Processing Unit	图形处理器
	Guest OS	Guest Operation System	客户操作系统（VM 内）
25	HC	Heterogeneous Computing	异构计算
26	HMI	Human Machine Interface	人机界面接口
27	HSM	分层存储管理	分级密钥管理
28	ICT	Information and Communication Technology	信息通信技术
29	ID2	Internet Device ID	物联网设备的可信身份标识
30	IEC	International Electrotechnical Commission	国际电工委员会
31	IoT	The Internet of Things	物联网
32	IPS/IDS	Intrusion Prevention System/ Intrusion Detection Systems	入侵检测和防护系统
33	Intel SGX	Intel Software Guard Extensions	Intel 指令集扩展
34	LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
35	MAC	Media Access Control Address	物理地址
36	MDE	Model-Driven Engineering	模型驱动
37	MEC	Multi-access Edge Computing	多接入边缘计算
38	MES	Manufacturing Execution System	制造执行系统

序号	中文名称	英文名称	中文名称
39	NAC	Network Access Control	终端网络安全准入系统
40	NFC	Near Field Communication	近场通信
41	NPU	Neural-network Processing Unit	嵌入式神经网络处理器
42	OA	Office Automation	办公自动化
43	OBD	On-Board Diagnostics	车载自诊断系统
44	OS	Operating System	操作系统
45	OT	Operation Technology	运营技术
46	PLC	Programmable Logic Controller	可编程控制器
47	RF	Radio Frequency	无线射频
48	SSL	Secure Sockets Layer	安全套接层
49	TCP/IP	Transmission Control Protocol/Internet Protocol	传输控制协议 / 网际协议
50	TLS	Transport Layer Security Protocol	安全传输协议
51	TEE	Trusted execution environment	可信执行环境
52	TPM	Trusted Platform Module	安全芯片
53	TSN	Time-Sensitive Networking	实时网络
54	USB	Universal Serial Bus	通用串行总线
55	VM	Virtual Machine	虚拟机
56	VLAN	Virtual Local Area Network	虚拟局域网
57	VPN	Virtual Private Network	虚拟专用网络
58	VR	Virtual Reality	虚拟现实
59	WPA2	Wi-Fi Protected Access	Wi-Fi 保护访问



附录 3

参考文献

[1] 中国工业互联网安全态势报告 (2018 年)[J]. 中国信息安全 , 2019(06):62-65.

[2] 边缘计算产业联盟 . 边缘计算参考架构 3.0, 边缘计算产业联盟白皮书 , 2018. 11. 30.

[3] 施巍松，刘芳，孙辉，裴庆祺 . 边缘计算 : Edge Computing. 北京 : 科学出版社 , 2018.

[4] 尚文利，赵剑明，刘贤达，尹隆，曾鹏 . 边缘计算信息安全需求与关键技术 . 自动化博览第四辑，2017, 11: 98-101.

[5] Stojmenovic, I., Wen, S.: The fog computing paradigm: Scenarios and security issues. In: FedCSIS. IEEE (2014)

[6] Zhang P, Liu J K , Yu F R, et al. A Survey on Access Control in Fog Computing[J]. IEEE Communications Magazine, 2017, 56(2):144-149.

[7] He T , Ciftcioglu E N, Wang S, et al. Location Privacy in Mobile Edge Clouds: A Chaff-Based Approach[J]. IEEE Journal on Selected Areas in Communications, 2017, 35(11):2625-2636.

[8] Antonio C, Maria F, Antonino G, et al. An approach for the secure management of hybrid cloud-edge environments [J]. Future Generation Computer Systems, 2018.

[9] Dubey, H., Yang, J., Constant, N., Amiri, A.M., Yang, Q., Makodiya, K.: Fog data: enhancing telehealth big data through fog computing. In: Proceedings of the ASE BigData & SocialInformatics. ASE BD&SI 2015, pp. 14:1–14:6 (2015).

[10] An X, Su J, Lü X, et al. Hypergraph clustering model-based association analysis of DDOS attacks in fog computing intrusion detection system[J]. EURASIP Journal on Wireless Communications and Networking, 2018, 2018(1): 249.

关注边缘计算产业联盟
请扫二维码

边缘计算产业联盟（ECC）

地址：北京市海淀区上地十街辉煌国际 5 号楼 1416
邮编：100085
网址：www.ecconsortium.net
邮箱：info@ecconsortium.net
电话：010-62669087

工业互联网产业联盟

地址：北京市海淀区花园北路 52 号
邮编：100191
网址：http://www.aii-alliance.org
邮箱：aii@caict.ac.cn
电话：010-62305887